

DOSSIER DE SYNTHESE DE PRATIQUE PROFESSIONNELLE (DSPP)

Technicien **S**upérieur en **R**éseaux
Informatiques et **T**élécommunications
d'**E**ntreprise (TSRITE)

Association **N**ationale pour la **F**ormation
Professionnelle des **A**dultes (AFPA)

19 Avenue de l'observatoire, 25000 Besançon

Responsable de formation :

M. Yannick KOHLER

Stagiaire :

M. Olivier HOUBLOUP



gagnez en **compétences**

Année 2008-2009

REMERCIEMENTS

Je tiens ici à remercier toutes les personnes qui m'ont encouragé lors de cette année et qui ont ainsi participé à la bonne réussite, d'une manière ou d'une autre, de ma reconversion professionnelle.

A Messieurs Yannick KOHLER et Philippe QUARREY, respectivement formateur TSRITE et TSGRI à l'AFPA de Besançon, pour toute leur contribution à ma réussite professionnelle et leurs encouragements dans ce domaine vaste qu'est l'informatique de réseau. Je les remercie aussi pour leur professionnalisme dans le partage des connaissances, pour leur patience et leur disponibilité.

SOMMAIRE

REMERCIEMENTS	1
SOMMAIRE	2
FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 1	8
Mettre en exploitation et garantir la continuité de service des réseaux informatiques et télécommunications de l'entreprise.....	8
FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 2	13
Contribuer à l'administration des réseaux informatiques et télécommunications d'entreprise ..	13
FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 3	21
Participer aux études d'optimisation des réseaux informatiques et télécommunication d'entreprise.....	21
TABLES DES MATIERES	26
ANNEXES	28



Nom patronymique : HOUBLoup

Nom marital :

Prénom : OLIVIER

Adresse : RUE DE LA PLAN FENETTE
73480 BESSANS

DOSSIER DE SYNTHÈSE DE PRATIQUE PROFESSIONNELLE (DSPP)

Titre professionnel visé (intitulé) :

***TSRITE –Technicien Supérieur en Réseaux
Informatiques et Télécommunications d’Entreprise.***

Votre objectif est d’obtenir un titre professionnel délivré par le ministère chargé de l’emploi soit par la VAE (cocher la case), soit par la formation (cocher la case).

☐ **Validation des Acquis de l’Expérience (VAE)**

Vous avez reçu la décision de recevabilité de la DDTEFP. Vous devez maintenant préparer votre parcours de validation. Pour cela, vous devez compléter ce dossier qui sera soumis au jury. Vous y décrirez votre pratique professionnelle et, à partir des informations fournies, le jury évaluera vos acquis par rapport aux compétences requises du titre que vous souhaitez obtenir. Votre intérêt est donc de remplir ce dossier avec le plus grand soin afin de mettre en valeur votre expérience.

Pour compléter ce document, vous devez vous reporter au mode d’emploi ci-joint. Vous y décrirez de manière détaillée vos activités professionnelles à partir d’exemples concrets mettant en valeur votre pratique professionnelle.

Vous pouvez bénéficier d’un accompagnement pour vous aider à constituer ce dossier. La demande d’accompagnement est à adresser au centre qui organisera votre session de validation.

Vous avez aussi la possibilité de fournir à l’accompagnateur et au jury des preuves concrètes de votre activité professionnelle qui illustreront les informations

portées dans le dossier. Ces preuves pourront se présenter sur tout support (pièce, dossier, photos...).

☒ Parcours de formation

Vous avez effectué des activités professionnelles soit avant d'entrer en formation, soit au cours de votre formation elle-même, lors d'une période d'application en entreprise ou dans votre organisme de formation. Vous devez compléter ce dossier afin de présenter et de valoriser ce que vous avez mis en pratique durant ces expériences.

Ce document est complété avec l'aide du formateur, tout au long du parcours de formation. Le dossier est renseigné sous la responsabilité de l'organisme avec lequel a été signé le contrat de stage. Au cas où le parcours est réalisé dans différents organismes de formation, chacun de ces organismes doit s'assurer que le dossier décrit bien la pratique professionnelle du candidat pour la partie du parcours effectué sous sa responsabilité.

A partir de ces informations, le jury évaluera les compétences que vous avez acquises au cours de cette période.

- PRESENTATION DU DOSSIER -

Ce dossier reste votre propriété.

Vous pouvez le **compléter** durant tout votre parcours de certification.

Vous devez le conserver et le présenter obligatoirement à chaque étape de la certification.

Ce dossier comporte :

UNE FICHE DESCRIPTIVE, de deux pages, destinée à présenter votre pratique professionnelle pour chaque activité type du titre visé. Cette fiche est à reproduire et à compléter en autant d'exemplaires que le titre contient d'activités types ;

UN MODE D'EMPLOI pour remplir la fiche, accompagné d'un exemple

UN TABLEAU à renseigner si vous possédez une certification, un diplôme, ou un CQP proche de tout ou partie du titre visé

UNE DECLARATION SUR L'HONNEUR à formuler lors de l'élaboration du dossier et à compléter, le cas échéant, avec la liste des éléments ajoutés au dossier initial en cas de parcours progressif vers le titre

Ce dossier doit être présenté **agrafé** ou **relié**
Les fiches doivent être **numérotées à la main**

DIPLOMES, TITRES OU CERTIFICATS PRECEDEMMENT OBTENUS ET PROCHES DU TITRE PROFESSIONNEL VISE

(À remplir le cas échéant)

Indiquez dans le tableau ci-dessous le ou les certificats et/ou diplômes que vous avez déjà obtenus et qui sont proches du domaine professionnel du titre que vous souhaitez obtenir.

Ils pourront, si l'arrêté de spécialité créant le titre professionnel que vous visez prévoit une équivalence, vous permettre d'alléger vos modalités d'évaluation et augmenter vos chances de réussite.

Cette information communiquée au jury est donc importante.

Intitulé de la certification obtenue (Titre, diplôme, CQP...)	Autorité ayant délivré la certification (Ministère, branche professionnelle...)	Date d'obtention

- DECLARATION SUR L'HONNEUR -

Elle garantit l'authenticité des informations et documents du dossier.

Elle doit être nominative, datée et signée.

Déclaration sur l'honneur du (de la) candidat(e)

Je soussigné(e) déclare sur
l'honneur de l'exactitude des renseignements fournis dans ce dossier et
être l'auteur des réalisations jointes en annexe.

Fait à , le

Pour faire valoir ce que de droit.

(Signature)

En cas de réussite partielle au titre (obtention de CCP), votre parcours de certification s'effectuera en plusieurs étapes sur une durée maximale de 5 ans.

Dans ce cas, vous pouvez ajouter à ce dossier initial des compléments et/ou modifications acquis ultérieurement. Il convient donc de les lister dans le tableau ci-dessous.

Liste des éléments ajoutés au dossier initial en cas de poursuite de votre parcours après une réussite partielle au titre (obtention de CCP)

- Candidats par VAE et par formation -

Liste des éléments ajoutés au dossier	Dates	Signature

FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 1

Intitulé de l'activité-type :

Mettre en exploitation et garantir la continuité de service des réseaux informatiques et télécommunications de l'entreprise

1 Indiquez les résultats directs de votre action : produits fabriqués, ouvrages, prestations de service ou autres productions que vous avez réalisés ou auxquels vous avez contribué

Montage, configuration et installation logiciel sur ordinateurs
Intégration des équipements d'interconnexion LAN et WAN
Réalisation de câbles
Travaux pratiques de l'académie CISCO : CCNA 1 et étude de cas
Réalisation de tâches quotidiennes d'exploitation
Contrôle de conformité d'un local technique
Exploitation d'équipement téléphonique
Assistance, conseil et assurance de support technique auprès de clients

2 Décrivez les tâches et/ou opérations que vous avez directement effectuées en vue des réalisations indiquées ci-dessus ainsi que leur fréquence de réalisation

Montage des éléments de base d'un ordinateur : disque dur, carte graphique, barrettes mémoires. Paramétrage de la station de travail en fonction des éléments
Connexion au réseau local et extérieur, à des commutateurs et à des concentrateurs et entre ordinateurs.
Réalisation de câble croisé à paires inversées et droit type RJ45
Connexion du matériel CISCO : routeur modèle Catalyst 2811, Switch modèle Catalyst 2960. Utilisation et paramétrage de routeurs CISCO en mode console.
Connexion des interfaces en mode console
Connexion des interfaces LAN d'un routeur
Connexion des interfaces WAN d'un routeur
Configuration du routeur à l'aide du SETUP
Établissement d'une session en mode console avec HyperTerminal
Utilisation des premières commandes (show running-config, show startup-config)

1. Sauvegarde de tout le système d'exploitation avec des logiciels. Exploitation des capacités de partitionnement des disques.

2. Formation audio visuelle à l'habilitation électrique en informatique et exploitation de celle-ci en situation concrète.
3. Travaux pratiques de téléphonie : liaison PABX, connexion et paramétrage des téléphones, utilisation de logiciels
4. Dépannage au sein de l'AFPA, évaluation des optimisations sur certaines stations de travail

Fréquence de réalisation :

☐ Très fréquemment ☒ Fréquemment ☐ Rarement

3 Lieux où cette pratique professionnelle a été exercée

Nom de l'entreprise, organisme ou association	Lieu	Chantier, atelier, services ou autres (à préciser)
Centre AFPA	Besançon 19 Avenue de l'observatoire Bâtiment N°14	Salle de travail pratique annuelle Local technique du bâtiment 14 Autres locaux AFPA lors des interventions

4 Indiquez la période de l'exercice de cette pratique professionnelle

Du 25 février 2008 au 11 juillet 2008

5 Précisez les moyens que vous avez utilisés pour accomplir les tâches décrites : matériels, outils, techniques, matériaux, produits, logiciels,...

Unités centrales type stations de travail

Switch catalyst 2960 et Hub CISCO, aide par Cisco pedia3.0

A partir d'un câble nu et de prises nues, montage, puis test avec un appareil spécifique

Utilisation du matériel de travaux pratique routeur 2811. Utilisation du logiciel de simulation de réseau packet tracer 5.0

Sauvegarde de tout le système d'exploitation avec des logiciels. Exploitation des capacités de partitionnement des disques.

Utilisation des logiciels de sauvegarde : Norton Ghost 12, PowerQuest, Drive Image XL.
Utilisation de logiciels de gravure (conjointement aux logiciels de sauvegarde) : Roxio créator 9.0 DE ; Nero 7 premium
Utilisation de logiciels de partitionnement et de rattrapage d'erreur : Partition Magic 8.0, compilation de logiciels de Hiren's Boot CD
Utilisation de logiciels d'optimisation : Diskeeper
Utilisation de logiciels de synchronisation : Goodsync, Toucan portable
Utilisation des logiciels de nettoyage : CCleaner, Spybots 1.6.0, ...
Utilisation de logiciels de protection : Avast antivirus, AVG free Antivirus.
Document écrit de synthèse et de normes.

Vidéos formatives.

Tests d'acquisition des connaissances.

Explication sur exemple concret au local technique de l'AFPA.

Intégration des données des connaissances par la présentation en trinôme de l'étude de cas CISCO (CCNA1) - cf. Annexe.

1. PABX e.volution (@dept telecom), poste dédié e.950, logiciel CTI manager
2. Savoir-faire et fiche technique d'intervention
3. Exploitation de l'anglais technique pour comprendre et utiliser des informations, des logiciels.
4. Introduction à Linux par l'installation d'un serveur Apache et utilisation de linux Ubuntu 8.04. Découverte de certaines commandes.

6 Pour la réalisation de ces tâches ou opérations, avez-vous travaillé seul ou en équipe, avec ou sans consignes, en relation avec d'autres personnes de votre entreprises ou extérieures à votre entreprise ...) ? Si oui, précisez dans quelles circonstances

La plupart des phases d'apprentissages personnels ont été effectuées en solo.

Lorsque j'ai recâblé toute la baie de brassage du local technique des formateurs TSRITE / TSGRI, j'ai effectué se travail, seul, à 90 %. Tout cette activité de référencement a été une manipulation personnelle, qui a été supervisé par mon formateur.

Les Travaux Pratiques ont été réalisés le plus possible en binôme.

L'étude de cas de CISCO (CCNA 1), a été réalisée en trinôme.

7 Documents annexes

7.1 Le cas échéant, documents prévus dans le règlement du titre visé

Aucun dans cette formation initiale.

7.2 Documents complémentaires en option

Indiquez ici la liste des documents que vous souhaitez présenter au jury.
Certaines productions ne sont pas facilement imprimables. Dans ce cas, j'en joins seulement des extraits.

ANNEXE 1

Etude de cas CISCO, CCNA 1 (Extrait)

ANNEXE 2

Mise à jour personnelle du local technique AFPA, bâtiment 14. (Extrait)

ANNEXE 3

Amélioration et synthèse d'une procédure pour récupérer la configuration IOS d'un routeur

J'ai commencé ma formation à l'AFPA le 25 février 2008. C'est pour moi une totale reconversion professionnelle. A part mon expérience d'utilisateur d'un ordinateur, je n'ai guère de connaissances dans ce secteur nouveau qui m'attire beaucoup.

Dans un premier temps, j'ai mis à jour et parfait mes connaissances par des travaux pratiques sur Microsoft Word, puis Microsoft Excel, tout en passant progressivement de la version 2003 à 2007. Ensuite, très vite, j'ai commencé à apprendre les données des cours CISCO.

Au fur et à mesure de la progression du groupe, notre formateur a introduit de nouvelles connaissances, plus ou moins directement liées à notre futur métier. J'ai vu l'algèbre de Boole, les tableaux de Karnaugh, les notions de logique en électricité, les équations logiques (*et, ou, et non, ou non*), différents théorèmes et les conversions dans les différentes bases (binaire, décimale, octale, hexadécimale).

Cela nous a permis d'acquérir une base de connaissances mais aussi une manière de réfléchir et d'aborder par la suite des notions d'algorithmes et de programmes. Cela a été vu sous Linux, avec notamment des commandes nouvelles pour moi.

Dans ce même temps ont été aussi abordés les diagrammes de GANTT, que ce soit sur papier ou avec le logiciel Microsoft Project 2007. A mon avis, ces notions nous seront très utiles par la suite dans notre métier. La prévision de réalisation de tâches pour le bon déroulement d'un projet est courante dans mon futur métier.

Durant cette première activité, j'ai aussi été curieux de logiciels informatiques non spécifiquement en rapport direct avec notre formation. Ceux-ci m'ont permis de renforcer certaines manières d'agir face à un problème et de développer le goût de la recherche dans différents axes : par exemple, les logiciels utilisés pour « écouter le réseau ». Formés en général à savoir nous protéger des intrusions et de l'espionnage, nous ne le sommes pas forcément à voir comment et avec quoi des gens malveillants tentent de contourner les failles du réseau.

A titre privé, j'ai déjà aidé des personnes novices en informatique. Cela diffère certes des connaissances pointues des réseaux ou de la téléphonie, mais c'est très intéressant de savoir expliquer et de se faire comprendre pour transmettre avec des mots simples des notions extérieures au quotidien de vie de certaines personnes. Idem avec des dépannages et des initiations à l'informatique à des non-initiés.

Soucieux de mettre en pratique mes connaissances, j'ai proposé à mon formateur (sous sa surveillance) de recâbler entièrement seul la baie de brassage de notre local technique, ainsi que de remettre à jour tout le listing de l'adressage IP. La phase de préparation, autant que celle des manipulations techniques, furent des moments très intéressants et tout à fait formateurs.

Je garde vraiment un très bon souvenir de toutes ces premières semaines. Ce fut aussi humainement enrichissant d'avoir été délégué du groupe TSRITE : la vision de l'Entreprise AFPA n'est pas la même, selon le degré d'implication.

Date : 28 janvier 2009

FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 2

Intitulé de l'activité-type :

Contribuer à l'administration des réseaux informatiques et télécommunications d'entreprise

1. Indiquez les résultats directs de votre action : produits fabriqués, ouvrages, prestations de service ou autres productions que vous avez réalisés ou auxquels vous avez contribué

Microsoft Windows server 2000 : installation, configuration et tests

Microsoft Windows server 2003 : installation, configuration et tests

Microsoft Windows exchange 2003 : installation, configuration et tests

Microsoft Windows server 2008 : installation, configuration mineure

Installation de Microsoft Windows server 2000 puis 2003 sur machines physiques, puis de manière virtuelle.

Virtualisation : exploitation du logiciel VMware 6

Linux ubuntu 7.04 et 8.04 : installation et configuration

Linux mandriva et linux debian : installation et découverte,

Microsoft Windows vista : installation, configuration et découverte

Travaux pratiques CISCO et mise en place d'un tutoriel vidéo pour toute la réalisation de l'étude de cas du CCNA2

2. Décrivez les tâches et/ou opérations que vous avez directement effectuées en vue des réalisations indiquées ci-dessus ainsi que leur fréquence de réalisation

1) Microsoft Windows server 2000 : installation, configuration et tests

- Installation et paramétrage du système d'exploitation Windows 2000 Pro à partir d'un CD bootable.
- Installation des pilotes des différents composants
- installation de Windows 2000 en mode Serveur Autonome à partir d'un CD ROM amorçable
- Compréhension de l'organisation des disques.
- Différentiation des disques de bases et des disques dynamiques / Avantages des disques dynamiques.
- Notions de volumes et de montage de volumes
- Différenciation entre les autorisations dans les systèmes de fichiers FAT et NTFS par rapport aux utilisateurs locaux et les utilisateurs distants.
- Conversion d'une partition FAT en une partition NTFS avec la commande convert.
- Installation d'un contrôleur de domaine

- Installation d'un serveur autonome (Workgroup) et le promouvoir en serveur membre d'un domaine
- Création des comptes utilisateurs dans Active Directory et attribution des paramètres personnels ainsi que des paramètres de Comptes
- Création d'un compte "Modèle" disposant de caractéristiques communes et utilisé pour créer un nombre important d'utilisateurs aux caractéristiques semblables.
- Reconnaissance des membres initiaux des groupes prédéfinis
- Création des groupes et ajout des utilisateurs.
- accès à des partages administratifs
- utilisation des permissions NTFS
- manipulation de la notion d'héritage des autorisations
- édition des permissions effectives lorsqu'un dossier possède les permissions de partage et des permissions NTFS.
- Gestion des permissions NTFS sur des fichiers après copie ou déplacement.
- création d'un répertoire de base pour un utilisateur et gestion des droits d'accès
- mise en place et stockage d'un profil errant pour un utilisateur "nomade". Test du téléchargement du profil.
- Création d'un profil qui s'applique à un ensemble d'utilisateurs, Rendre ce profil non modifiable
- installation d'un serveur d'impression
- manipulation des permissions, des restrictions et des priorités accordées à une imprimante
- définition des restrictions différentes sur des imprimantes différentes accédant au même périphérique d'impression.
- création d'une console de gestion permettant de gérer différents services de façon à obtenir une seule interface d'administration pour ces services
- mise en œuvre d'une topologie DFS autonome et y accéder
- Définition d'un quota de disque pour les utilisateurs
- mise en œuvre des protocoles et services réseau.
- utilisation des commandes permettant de tester la connectivité.
- analyse du trafic réseau.
- installation et configuration d'un serveur DHCP
- création des étendues d'adresses
- configuration d'un serveur DNS principal et activation des enregistrements dynamiquement.
- vérification du bon fonctionnement du serveur DNS.
- configuration d'un serveur WINS et d'un client WINS
- application des stratégies de groupes
 - o Sur Active Directory au niveau ordinateur ou au niveau utilisateur
 - o Sur un Site
 - o Sur un Domaine
 - o Sur une UO ou plusieurs UO imbriquées
- utilisation de l'Assistant de Sauvegarde pour sauvegarder et restaurer
 - o Les fichiers ou les lecteurs
 - o L'état du système (Active Directory)
- test des différents types de sauvegarde.

- Création et utilisation d'une disquette de réparation d'urgence.
- recherche, enregistrement et installation d'un service Pack.
- recherche, enregistrement et installation des Mises à jour (Update).
- recherche et installation des informations techniques et des outils supplémentaires
- utilisation des fonctionnalités principales de Terminal Server.
- installation et gestion du Terminal Server.
- installation et configuration du client Terminal Server.
- utilisation d'une Console de Gestion à distance en utilisant Terminal Server.
- création d'une panne par effacement volontaire de fichier important
- réparation une installation Windows 2000
 - o Utilisation du mode sans échec
 - o Installation et utilisation de la console de récupération
 - o Utilisation de la disquette de récupération

2) Microsoft Windows server 2003 : installation, configuration et tests

Les mêmes manipulations que pour Microsoft Windows server 2000, avec toute la notion d'adaptation car évolutions logiciels.

3) Microsoft Windows exchange 2003 : installation, configuration et tests

Création de compte utilisateur en local et tests d'envoi / réception de mails. Paramétrage divers pour comprendre le logiciel

4) Microsoft Windows server 2008 : installation, configuration mineure

Comme pour Microsoft Windows server 2000 sauf que nous n'avons pas pu avancer très loin : installation et petite configuration seulement.

Création de l'Active Directory, création serveur DNS, Création serveur DHCP, Création d'un serveur d'impression.

Test de connectivité entre utilisateurs d'un même domaine mais avec une station sous Windows 2000 pro, une station sous windows 2003, une station sous windows XP, une station sous linux Ubuntu 8.04

Apprentissage des paramétrages des différentes stations de travail.

5) et 6) Installation de Microsoft Windows server 2000, puis 2003 sur machines physiques, et enfin de manière virtuelle.

Après avoir effectué toutes ces manipulations sur des serveurs et des stations de travail physique, nous avons testé sur un ordinateur des machines virtuelles.

Il y a eu connectivité entre les machines virtuelles du même ordinateur : Microsoft Windows server 2000, 2003 et Windows 2003 en station utilisateurs.

Il y a aussi eu connectivité entre les machines virtuelles et le serveur physique sous Microsoft Windows server 2008

6) et 8) Installation et configuration de différentes versions de Linux, en suivant les tutoriels et en appliquant nos connaissances sous Microsoft Windows. Paramétrage simple pour la connectivité entre PC et vers Internet. Pas encore de paramétrages spécifiques comme ceux des administrateurs réseau.

Découvertes en mode utilisateurs et apprentissage de certaines options diverses.

Installation des mises à jour en ligne de commandes.

Utilisation des lignes commandes pour d'autres actions : gestions des fichiers et dossiers, reconnaissance et compréhension de l'arborescence

1) Microsoft Windows vista : installation, configuration et découverte

Installation sur une station de travail. Paramétrages divers. Connectivité à Internet. Comparaison par rapport à Windows XP. Compréhension des nouveautés et des changements.

Plusieurs réinstallations car trop « d'écrans bleus » sans réparation visible !

2) Travaux pratiques CISCO et mise en place d'un tutoriel vidéo pour toute la réalisation de l'étude de cas du CCNA2

Intégration et manipulations spécifiques exécutées lors des travaux pratiques de tout le CCNA 2 : autant sur les supports physiques (plusieurs routeurs reliés) que par émulation logiciel (Packet tracer 5.0)

- Connexion des interfaces en mode console
- Connexion des interfaces LAN d'un routeur
- Connexion des interfaces WAN
- Configuration d'un routeur à l'aide du setup
- Établissement d'une session en mode console avec HyperTerminal
- Principes fondamentaux de la ligne de commande
- Modes de commande et identification de routeur
- Configuration des mots de passe d'un routeur
- Utilisation des commandes show d'un routeur
- Configuration d'une interface série
- Modification d'une configuration
- Configuration d'une interface Ethernet
- Configuration des descriptions d'interface
- Configuration du message du jour (MOTD)
- Configuration des tables d'hôtes
- Sauvegarde des fichiers de configuration
- Création d'un schéma de réseau avec CDP
- Utilisation des commandes CDP
- Établissement et vérification d'une connexion Telnet
- Interruption et déconnexion de sessions Telnet
- Opérations Telnet avancées
- Tests de connectivité – Ping
- Tests de connectivité – Traceroute
- Dépannage des problèmes d'adresse IP
- Utilisation de la commande boot system
- Résolution des problèmes de démarrage liés au registre de configuration
- Gestion des fichiers de configuration avec TFTP
- Gestion des images de l'IOS avec TFTP
- Procédures de récupération de mot de passe
- Gestion des images de l'IOS avec ROMmon et Xmodem
- Configuration de routes statiques
- Configuration et dépannage du protocole RIP

- Empêcher les mises à jour du routage via une interface
- Équilibrage de charge sur plusieurs chemins
- Configuration du protocole IGRP
- Configuration du protocole OSPF
- Routage par défaut avec les protocoles RIP et IGRP
- Équilibrage de charge de coût différent avec IGRP
- Utilisation de la commande show ip route pour examiner les tables de routage
- Passerelle de dernier recours /passerelle de défaut
- Dernière mise à jour des routes
- Dépannage à l'aide des commandes ping et telnet
- Dépannage à l'aide de la commande traceroute
- Dépannage des problèmes de routage avec show ip route et show ip protocols
- Dépannage des problèmes de routage avec la commande debug
- Sessions d'hôtes actives multiples
- Numéros de ports bien connus et sessions multiples
- Configuration de listes de contrôle d'accès standard
- Configuration de listes de contrôle d'accès étendues et étendues simples
- Configuration de listes de contrôle d'accès nommées
- TP 11.2.3b Listes de contrôle d'accès étendues pour les zones DMZ (zones démilitarisées) simples
- Fonctions des listes de contrôle d'accès multiples
- Restrictions applicables aux terminaux virtuels (VTY)

Fréquence de réalisation :

☐ Très fréquemment

☒ Fréquemment

☐ Rarement

3. Lieux où cette pratique professionnelle a été exercée

Nom de l'entreprise, organisme ou association	Lieu	Chantier, atelier, services ou autres (à préciser)
Centre AFPA	Besançon 19 Avenue de l'observatoire Bâtiment N°14	Salle de travail pratique annuelle Local technique du bâtiment 14

4. Indiquez la période de l'exercice de cette pratique professionnelle

Du 02 juin 2008 au 20 juin 2008 : Travaux pratiques de téléphonie

Du 23 juin 2008 au 12 juillet 2008 : Linux (approfondissement)

Du 15 juillet 2008 au 1^{er} août 2008 : Microsoft Windows server 2000

Du 18 août 2008 au 22 août 2008 : Microsoft Exchange 2003

Du 25 août 2008 au 26 septembre 2008 : Microsoft Windows server 2003 + Microsoft Windows server 2008

Du 29 Septembre 2008 au 24 octobre 2008 : CISCO CCNA 2 et étude de cas sur le routage

5. Précisez les moyens que vous avez utilisés pour accomplir les tâches décrites : matériels, outils, techniques, matériaux, produits, logiciels,...

Intégration des outils de sécurité et d'administration réseau : logiciel de supervision « the dude », paramétrage routeur, paramétrage de pare-feu

Assurance de tâches d'administration des services réseaux standards (DHCP, DNS, http, SMTP). Surtout sous Microsoft Windows serveur 2000 et 2003

Proposition d'investissement réseau sur des commutateurs par le biais de catalogues techniques.

Référencement fréquent en matière de téléphonie et voix sur IP à la documentation de l'intervenant Rémy Lacroix (Orange Business Service). Intervention d'ailleurs sous forme de conférence d'une journée.

Exploitation de l'anglais technique pour comprendre et utiliser des informations, des logiciels. Entraînement à l'oral pour des conversations de type entretien d'embauche, dépannage aux utilisateurs.

6. Pour la réalisation de ces tâches ou opérations, avez-vous travaillé seul ou en équipe, avec ou sans consignes, en relation avec d'autres personnes de votre entreprises ou extérieures à votre entreprise ...) ? Si oui, précisez dans quelles circonstances

La plupart des phases d'apprentissage personnel ont été réalisées en solo.

Les Travaux Pratiques ont été effectuées le plus possible en binôme.

Les échanges dans le groupe ont permis de nous entraider sur les manipulations lors des Travaux pratiques sur Microsoft Windows server 2000.

L'étude de cas de CISCO (CCNA 2), a été réalisée en solo, par mes soins.

7. Documents annexes

7.1. *Le cas échéant, documents prévus dans le règlement du titre visé*

Aucun dans cette formation initiale.

7.2. *Documents complémentaires en option*

Indiquez ici la liste des documents que vous souhaitez présenter au jury.
Certaines productions ne sont pas facilement imprimables. Dans ce cas, j'en joins seulement des extraits.

ANNEXE 4

Etude de cas CISCO, CCNA 2. Le routage. (Extrait)

J'ai commencé très naturellement l'activité 2 à la suite de la première et celle-ci m'a semblé dès le début approfondir les notions vues précédemment. En effet, les CCNA de l'entreprise CISCO permettent une approche générale des réseaux et des télécommunications. Plus nous avançons dans les chapitres, plus certaines notions sont reprises avec des détails supplémentaires.

Cette activité-type N°2 – Contribuer à l'administration des réseaux informatiques et télécommunication d'entreprise, représente une très importante partie de notre formation. J'ai eu la possibilité d'utiliser différents systèmes d'exploitation sur les ordinateurs : principalement Microsoft Windows server 2000 et Microsoft Windows server 2003 et aussi, mais plus brièvement, Linux avec la version Ubuntu 8.04.

Les travaux pratiques sous Microsoft Windows server 2000 ont occupé une grande partie de mon temps. Les manipulations, dont les difficultés étaient croissantes, m'ont permis de découvrir des paramétrages très précis. J'ai aussi essayé, quand cela était possible, d'effectuer les mêmes manipulations sous Microsoft Windows server 2003. J'ai constaté des différences et des améliorations dans l'ergonomie et les facilités de la version 2003. Bien que nous n'ayons pas de travaux pratiques pour la version 2003, j'ai pris l'initiative de la réalisation : curiosité de ma part et constat de fort abandon de la version 2000 par les entreprises. Et j'ai eu un peu de temps pour procéder de même avec la version 2008.

La phase des activités du CCNA 2 m'a bien plu car je l'ai trouvée très intéressante sur la réflexion - surtout lors de l'étude de cas. J'ai pris le temps de peaufiner tout mon travail et de créer en plus un tutoriel précis sous forme vidéo avec des commentaires écrits. (Cf. annexes)

Sur le bilan des actions menées lors de cette deuxième période de formation, je me suis rendu compte que j'ai déployé de plus en plus les compétences demandées. J'ai axé un peu plus précisément sur l'intégration, le paramétrage et l'exploitation des outils de sécurité et d'administration réseau ; l'administration des infrastructures et de services réseaux et celle de services de messagerie unifiée.

Au fur et à mesure de ma formation, je confirme que j'apprécie de résoudre des difficultés techniques, surtout en situation de cas concrets.

Date : 28 janvier 2009

FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 3

Intitulé de l'activité-type :

Participer aux études d'optimisation des réseaux informatiques et télécommunication d'entreprise

1. Indiquez les résultats directs de votre action : produits fabriqués, ouvrages, prestations de service ou autres productions que vous avez réalisés ou auxquels vous avez contribué

Travaux pratiques de l'académie CISCO : CCNA 1 et étude de cas

Travaux pratiques de l'académie CISCO : CCNA 2 et étude de cas

Travaux pratiques de l'académie CISCO : CCNA 3

Examens de Fin d'Activité 3 (EFA 3) - Etat de l'art sur les plans de reprise après sinistre

Plan de Reprise d'Activité Informatique (PRAI) lors de la Période d'Application en Entreprise (PAE).

2. Décrivez les tâches et/ou opérations que vous avez directement effectuées en vue des réalisations indiquées ci-dessus ainsi que leur fréquence de réalisation

Les actions menées lors des études de cas CISCO sont transversales entre les activités-types N°1, N°2 et N°3. Pour cette raison, je ne répète pas les données précédemment énoncées, même si toutes celles-ci s'intègrent parfaitement aux études d'optimisation des réseaux informatiques et télécommunications d'entreprise.

Au sujet de l'Examen de Fin d'Activité 3 (EFA 3), j'ai établi un état de l'art sur les plans de reprise après sinistre (méthodologie existante, contenu, portée). Ensuite, d'après l'état de l'art, j'ai choisi une méthodologie pour élaborer une stratégie de reprise après sinistre. J'ai présenté ce travail via un vidéoprojecteur ce travail.

La Période d'Application en Entreprise (PAE, est en continuité de l'EFA 3. Mon sujet de stage a concerné la mise en place d'un Plan de Reprise d'Activité Informatique après sinistre.

J'ai aussi eu l'occasion avec mon tuteur de stage de remonter un réseau complet de plusieurs serveurs sous Microsoft Windows server 2003.

Fréquence de réalisation :

☐ Très fréquemment

☒ Fréquemment

☐ Rarement

3. Lieux où cette pratique professionnelle a été exercée

Nom de l'entreprise, organisme ou association	Lieu	Chantier, atelier, services ou autres (à préciser)
Centre AFPA	Besançon 19 Avenue de l'observatoire Bâtiment N°14	Salle de travail pratique annuelle Local technique du bâtiment 14
Direction Régionale et Départementale de la Jeunesse et des Sports	27 Rue Alfred-Sancey 25000 Besançon	Service informatique Actions dans tout le bâtiment, composé de trois niveaux. Plus de 50 salles.

4. Indiquez la période de l'exercice de cette pratique professionnelle

Du 25 février 2008 au 11 juillet 2008 : CISCO CCNA 1 et étude de cas

Du 29 Septembre 2008 au 24 octobre 2008 : CISCO CCNA 2 et étude de cas sur le routage

Du 27 octobre 2008 au 1er décembre 2008 : CISCO CCNA 3

Du 27 octobre 2008 au 22 novembre 2008 : Examens de Fin d'Activité 3 (EFA 3) - plan de secours informatique

Du 24 novembre 2008 au 24 janvier 2009 : PRAI - Période d'Activité en Entreprise (PAE)

5. Précisez les moyens que vous avez utilisés pour accomplir les tâches décrites : matériels, outils, techniques, matériaux, produits, logiciels,...

Examens de Fin d'Activité 3 (EFA 3) : Etat de l'art sur les plans de reprise après sinistre :

Après avoir effectué une recherche documentaire sur les différentes méthodes et applications des plans de reprise, j'ai élaboré un plan de reprise du local technique de l'AFPA, bâtiment 14. Je ne me suis cependant pas allé jusqu'au bout de la démarche, car la compréhension de la notion de plan de reprise est vraiment une activité très vaste et un peu difficile.

Période d'Activité en Entreprise (PAE) : Création d'un Plan de Reprise d'Activité Informatique :

J'ai notamment utilisé des logiciels permettant d'analyser les réseaux : The Dude 3.0 beta8 et AutoScan Network 1.32.

Lors de la création du schéma du réseau, j'ai utilisé Microsoft Visio 2007.

Pour les autres parties, j'ai utilisé mes connaissances. Toute la partie de recherche d'informations sur la construction d'un PRAI a été effectuée par la consultation de documents d'organismes spécialisés, tel le Club de la Sécurité Informatique Français (CLUSIF).

J'ai aussi consulté la documentation technique propre au matériel utilisé. (Serveurs, stations de travail, copieurs multifonctions). Pendant cette période de stage, les serveurs étaient sous Microsoft Windows server 2003, tandis que les utilisateurs que j'ai dépannés pour le réseau travaillaient sous les versions Microsoft Windows 2000 et XP.

6. Pour la réalisation de ces tâches ou opérations, avez-vous travaillé seul ou en équipe, avec ou sans consignes, en relation avec d'autres personnes de votre entreprises ou extérieures à votre entreprise ...) ? Si oui, précisez dans quelles circonstances

La quasi-totalité des Travaux pratiques (hors étude de cas) a été réalisée en binôme, quand cela a été possible. Sinon j'ai travaillé en autonomie.

Pour le travail pratique de l'académie CISCO (CCNA 1 - étude de cas), nous étions en trinôme avec des consignes de projet.

Pour le travail pratique de l'académie CISCO (CCNA 2 - étude de cas), je l'ai effectué tout seul.

Pour mon Examen de Fin d'Activité 3 (EFA 3) sur l'état de l'art sur les plans de reprise après sinistre, j'étais seul à sa réalisation. J'ai suivi les consignes de la démarche de l'examen.

Pour le Plan de Reprise d'Activité Informatique (PRAI) lors de la Période d'Application en Entreprise (PAE), mon responsable de stage a supervisé mes manipulations car nous devons remonter le réseau de la DRDJS dans l'urgence. Ensuite, pour toutes les phases d'assistance aux utilisateurs, une fois la démarche acquise après démonstration, j'étais autonome.

7. Documents annexes

7.1 Le cas échéant, documents prévus dans le règlement du titre visé

Aucun dans cette formation initiale.

7.2 Documents complémentaires en option

Indiquez ici la liste des documents que vous souhaitez présenter au jury.
Certaines productions ne sont pas facilement imprimables. Dans ce cas, j'en joins seulement des extraits.

ANNEXE 5

Etat de l'art sur les plans de reprise après sinistre (EFA 3) - (extrait)

ANNEXE 6

L'emploi type de TSRITE

L'emploi type de TSGRI

Réussite aux examens du CCNA 1 et CCNA 2

Réussite aux Examens de Fin d'Activité (EFA) N°1, N°2 et N°3.

Cette activité-type, intitulée Participer aux études d'optimisation des réseaux informatiques et télécommunication d'entreprise, m'a offert la possibilité de synthétiser mes connaissances théoriques et pratiques afin de les utiliser dans des exemples de cas concrets.

C'est une phase intéressante de rassemblement d'acquis, ajoutée à une prise de maturité dans le choix des décisions et des optimisations.

J'ai surtout pu mesurer cela lors du stage en entreprise. Les incidents techniques qui sont apparus nous ont laissé une marge d'erreur faible. La situation était critique, sans être pour autant impossible à résoudre, mais nous devons travailler et réagir vite et bien. Il a fallu améliorer le service de réseau offert pour assurer les communications entre utilisateurs et optimiser son fonctionnement pour nous éviter de devoir recommencer des manipulations fastidieuses. J'ai travaillé en équipe avec mon responsable de stage quand les actions étaient trop sensibles et en autonomie lorsqu'il n'y avait pas de risque.

Aussi, pour la création du Plan de Reprise d'Activité Informatique (PRAI), ai-je cherché des pistes d'optimisation en fonction de nos moyens alloués présents et de ceux prochainement exploitables. Proposer des scénarios d'évolution du réseau, pour anticiper un plan de secours informatique, n'est pas évident. Cela fait appel à des connaissances professionnelles expertes, que l'on ne possède pas forcément tout de suite. Pour penser très loin, assurer la veille technologique, il faut de l'expérience et une capacité à ne pas s'emballer sur une technologie nouvelle. Il serait dommage de faire « machine arrière » peu de temps après. Cela. Néanmoins cela est très intéressant de chercher des solutions, même si toutes n'aboutissent pas.

En outre, j'ai dû faire face à des contraintes diverses : d'environnement (architecture technique principalement), d'organisations (budget du service informatique surtout) et de positionnement de l'entreprise (déménagement et politique de gestion incertaine).

Lors du stage, j'ai aussi composé entre la mission pour l'entreprise et celle de la rédaction du rapport de stage pour l'AFPA, le tout agrémenté de pannes techniques et donc d'un volume horaire ad hoc. La bonne gestion du temps a été un élément clé pour tout mener au mieux.

C'est sur cet exemple qu'il est important de comprendre que les propositions au niveau des technologies nouvelles dans une entreprise doivent être cohérentes avec les soutiens logistiques et leurs suivis par les acteurs informatiques. Il faut arriver à définir, par exemple, les réels besoins à venir et aussi leurs indicateurs de réussite. Savoir si la politique informatique sera cohérente avec la demande future est un travail de mûre réflexion et de forte projection.

Même si toutes ces démarches ne sont pas forcément simples, elles n'en sont pas moins intéressantes et très formatrices.

Date : 28 janvier 2009

TABLES DES MATIERES

REMERCIEMENTS	1
SOMMAIRE	2
FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 1	8
Mettre en exploitation et garantir la continuité de service des réseaux informatiques et télécommunications de l'entreprise.....	8
1 Indiquez les résultats directs de votre action : produits fabriqués, ouvrages, prestations de service ou autres productions que vous avez réalisés ou auxquels vous avez contribué	8
2 Décrivez les tâches et/ou opérations que vous avez directement effectuées en vue des réalisations indiquées ci-dessus ainsi que leur fréquence de réalisation.....	8
3 Lieux où cette pratique professionnelle a été exercée.....	9
4 Indiquez la période de l'exercice de cette pratique professionnelle	9
5 Précisez les moyens que vous avez utilisés pour accomplir les tâches décrites : matériels, outils, techniques, matériaux, produits, logiciels,... ..	9
6 Pour la réalisation de ces tâches ou opérations, avez-vous travaillé seul ou en équipe, avec ou sans consignes, en relation avec d'autres personnes de votre entreprises ou extérieures à votre entreprise ...) ? Si oui, précisez dans quelles circonstances	10
7 Documents annexes	11
7.1 Le cas échéant, documents prévus dans le règlement du titre visé	11
7.2 Documents complémentaires en option	11
FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 2	13
Contribuer à l'administration des réseaux informatiques et télécommunications d'entreprise ..	13
1. Indiquez les résultats directs de votre action : produits fabriqués, ouvrages, prestations de service ou autres productions que vous avez réalisés ou auxquels vous avez contribué	13
2. Décrivez les tâches et/ou opérations que vous avez directement effectuées en vue des réalisations indiquées ci-dessus ainsi que leur fréquence de réalisation.....	13
3. Lieux où cette pratique professionnelle a été exercée.....	17
4. Indiquez la période de l'exercice de cette pratique professionnelle	18
5. Précisez les moyens que vous avez utilisés pour accomplir les tâches décrites : matériels, outils, techniques, matériaux, produits, logiciels,... ..	18
6. Pour la réalisation de ces tâches ou opérations, avez-vous travaillé seul ou en équipe, avec ou sans consignes, en relation avec d'autres personnes de votre entreprises ou extérieures à votre entreprise ...) ? Si oui, précisez dans quelles circonstances	18
7. Documents annexes	19
7.1. Le cas échéant, documents prévus dans le règlement du titre visé	19

7.2. Documents complémentaires en option	19
FICHE DESCRIPTIVE DE LA PRATIQUE PROFESSIONNELLE CORRESPONDANT A L'ACTIVITE TYPE N° 3	21
Participer aux études d'optimisation des réseaux informatiques et télécommunication d'entreprise.....	21
1. Indiquez les résultats directs de votre action : produits fabriqués, ouvrages, prestations de service ou autres productions que vous avez réalisés ou auxquels vous avez contribué	21
2. Décrivez les tâches et/ou opérations que vous avez directement effectuées en vue des réalisations indiquées ci-dessus ainsi que leur fréquence de réalisation.....	21
3. Lieux où cette pratique professionnelle a été exercée.....	22
4. Indiquez la période de l'exercice de cette pratique professionnelle	22
5. Précisez les moyens que vous avez utilisés pour accomplir les tâches décrites : matériels, outils, techniques, matériaux, produits, logiciels,... ..	23
6. Pour la réalisation de ces tâches ou opérations, avez-vous travaillé seul ou en équipe, avec ou sans consignes, en relation avec d'autres personnes de votre entreprises ou extérieures à votre entreprise ...) ? Si oui, précisez dans quelles circonstances	23
7. Documents annexes	24
TABLES DES MATIERES	26
ANNEXES	28

ANNEXES

ANNEXE N° 1 :

Extraits de notre étude de cas CISCO, CCNA 1

ANNEXE N° 2 :

Mise à jour personnelle du local technique AFPA, bâtiment 14. (Extrait)

ANNEXE N° 3 :

Amélioration et synthèse d'une procédure pour récupérer la configuration IOS d'un routeur

ANNEXE N° 4 :

Etude de cas CISCO, CCNA 2. Le routage. (Extrait)

ANNEXE N° 5 :

Etat de l'art sur les plans de reprise après sinistre (EFA 3) - (extrait)

ANNEXE N° 6 :

L'emploi type de TSRITE

L'emploi type de TSGRI

Réussite aux examens du CCNA 1 et CCNA 2

Réussite aux Examens de Fin d'Activité (EFA) N°1, N°2 et N°3

ANNEXE 1

**Etude de cas CISCO, CCNA 1
(Extrait)**

Conception du réseau informatique

Etude de cas 1 :

Table des matières

1. Historique de l'organisation et état actuel.....	2
2. Prévisions de croissance	2
3. Politiques d'exploitation et procédures de gestion	2
3.1 Ressources et contraintes	2
3.1.1 Ressources matérielles :.....	2
3.1.2 Ressources humaines :	2
4. Systèmes et procédures d'administration	3
5. Points de vue des futurs utilisateurs du réseau local.	3
6. Journal technique :.....	4
3.2 Détermination des locaux informatiques.....	4
7. Topologie logique	7
3.3 Topologie du réseau :	7
8. Topologie physique	7
3.4 Type de câblage :	7
3.1.3 Câblage horizontal :.....	7
3.1.4 Câblage vertical :	8
3.1.5 Détails des éléments :	8
9. Matrices de résolution de problèmes.....	11
10. Récapitulatif des prises et des câbles, ...	11
11. Récapitulatif des équipements de réseau, des adresses MAC et des adresses IP.	11

1. **Historique de l'organisation et état actuel**

Le réseau à concevoir est réparti sur trois bâtiments distincts avec des spécificités différentes.
Les locaux sont neufs et prêts à être aménagés.

Plan des locaux en ANNEXES

2. **Prévisions de croissance**

Nous prévoyons une pérennité du réseau sur une période maximum de 20 ans.

L'évolutivité des postes de travail est à prendre en compte. Du point de vue du nombre de postes et de leur évolution technologique.

Doit s'en suivre un matériel adéquat ne nécessitant pas de grands changements et travaux successifs.

3. **Politiques d'exploitation et procédures de gestion**

Il s'agit de bâtiments d'un campus de type administratif.

3.1 **Ressources et contraintes**

3.1.1 **Ressources matérielles :**

Nous disposons d'un financement non limité mais dans le cadre d'un budget concret.

Il s'agit de prendre du matériel à des prix courants et réels.

Au niveau logiciel, aucune contrainte particulière.

3.1.2 **Ressources humaines :**

Il y aura au minimum 204 utilisateurs prévus.

Nous supposons qu'il y aura un administrateur réseau et deux techniciens de maintenance informatique.

Nous supposons que les utilisateurs aux postes de travail n'ont pas de connaissances pour une gestion de pannes quelconques en rapport avec le réseau.

Aussi, plusieurs secteurs d'administrations distincts nécessiteront une gestion particulière.

Au niveau de la gestion, outre les différents secteurs administratifs, les ennuis techniques ne devront pas perturber l'ensemble du réseau, mais le minimum possible.

De même, une gestion indépendante, pour des raisons de sécurité des données devra être établie inter et extra-secteurs.

4. Systèmes et procédures d'administration

Le parc informatique sera géré par des administrateurs systèmes capable d'utiliser différentes technologies informatiques. Le matériel, de type professionnel, devra permettre une administration de type Unix et/ou Microsoft.

Fonctionnement du LAN :

Toutes les références données concernant des câbles sont choisies chez Legrand.

Chaque utilisateur, dans chaque salle, possèdera une connexion par câble RJ45 1Gbits/s.

Chaque PC, sera connecté aux blocs informatiques de 4 ports situés dans le mur.

Nous prévoyons une moyenne de 5m de câble, du PC vers le mur, dans la mesure où nous ignorons la superficie des pièces.

Derrière chaque bloc informatique, viendront se connecter 4 câbles F/STP cat 6. Ils iront jusqu'aux panneaux de brassage, de 48 ou 72 ports insérés dans un coffret de 12U par local technique.

En sortie du panneau de brassage viendront se loger à nouveau des blocs informatiques de 4 ports.

Puis par port des câbles RJ-45 1Gbits/s F/STP cat 6), de longueur de 3 mètres, se connecteront sur les ports des différents switches.

« Dans les locaux techniques contenant les 2 types de switches, ceux-ci s'interconnecteront entre eux via un kit de stack enfiché à l'arrière de chaque switch.(ref AX 742 netgear)

Le débit sera de 24Gbit/s via un cordon de 60cm fourni.

Après chaque local technique qui sera connecté, soit à un autre bâtiment soit à un autre local technique, le sera grâce à un module adaptateur 10 Gbits/s Ethernet XFP (ref : AX741 netgear) enfilé dans un slot à l'arrière du switch.

A l'intérieur de ce module viendra s'enfiler un transceiver XFP ethernet 10GBase-SR, dans lequel une fibre optique LC Duplex Multimode sera insérée.

Le modem routeur DGFV338 sera logé dans le POP, et relié au LAN via un câble 1Gbits/s, au local technique 'C', du rez-de-chaussée du bâtiment principale.

5. Points de vue des futurs utilisateurs du réseau local.

Besoins actuels et futurs :

Les futurs utilisateurs devront avoir accès aux données distantes de manière rapides et efficaces.

La prévision d'ajout de postes de travail aux deux initialement prévus, doit être prise en compte. Par exemple sur un doublement des effectifs et cela sans gêne d'accès aux données diverses.

6. Journal technique :

3.2 Détermination des locaux informatiques

Le choix d'un local technique doit tenir compte et être conforme à différentes normes.

		longueur (m)	largeur (m)	surface (m ²)	locaux retenus
Bâtiment principal	Rez-de-chaussée	40	37	1480	C ; F
	Premier étage	40	37	1480	I ; H
Bâtiment EST	Rez-de-chaussée	40	23	920	L
	1 ^{er} étage	40	23	920	Q
Bâtiment OUEST	Rez-de-chaussée	40	23	920	T
	1 ^{er} étage	40	23	920	W

Nous avons retenu pour le bâtiment principal les locaux C, F, J et H. sachant que ces derniers nécessitent des travaux préalables. Pour les autres bâtiments, les locaux L, Q, T, W répondent aux critères de sélection.

Le sol du local technique principal contenant le répartiteur principal doit supporter la charge indiquée dans les instructions d'installation fournies avec les équipements. La capacité minimale est de 4,8 kPa. Pour les locaux intermédiaires, le sol doit supporter une charge minimale de 2,4 kPa.

Sachant que la surface au sol recommandée est de 1000 m² par local technique, seul le bâtiment principal a besoin de 2 locaux techniques par étage, contre respectivement 1 pour les autres bâtiments, sachant que le rayon d'efficacité du local technique est de 50m.

- les matériaux des murs, du sol et des plafonds
- la température et l'humidité
- l'emplacement des appareils d'éclairage et leur type
- les prises de courant
- l'accès au local et à l'équipement
- l'accès aux câbles et leur support

En effet, ces locaux sont conformes aux exigences requises :

- Nombre de prises électriques minimum requis étant de 2.
- Eclairage incandescent (l'éclairage fluorescent produit des interférences électriques)
- ouverture extérieure (en cas d'incendie)
- Serrure (protection des intrusions)
- Plafond non suspendu
- Murs avec peinture ignifuge (incendie)

- Pas de canalisation d'eau
- Pas de produits chimiques toxiques
- Pas de présence de ligne principale d'alimentation en électricité (interférences électromagnétiques)

Travaux préalables du local H :

Suppression et remplacement de l'éclairage fluorescent par un éclairage incandescent.

Travaux préalables du local J :

Suppression et remplacement de l'éclairage fluorescent par un éclairage incandescent.

Changement du sens d'ouverture de la porte. De l'intérieur vers l'extérieur.

Ajouter un système de fermeture sécurisé au local.

Supprimer le plafond suspendu.

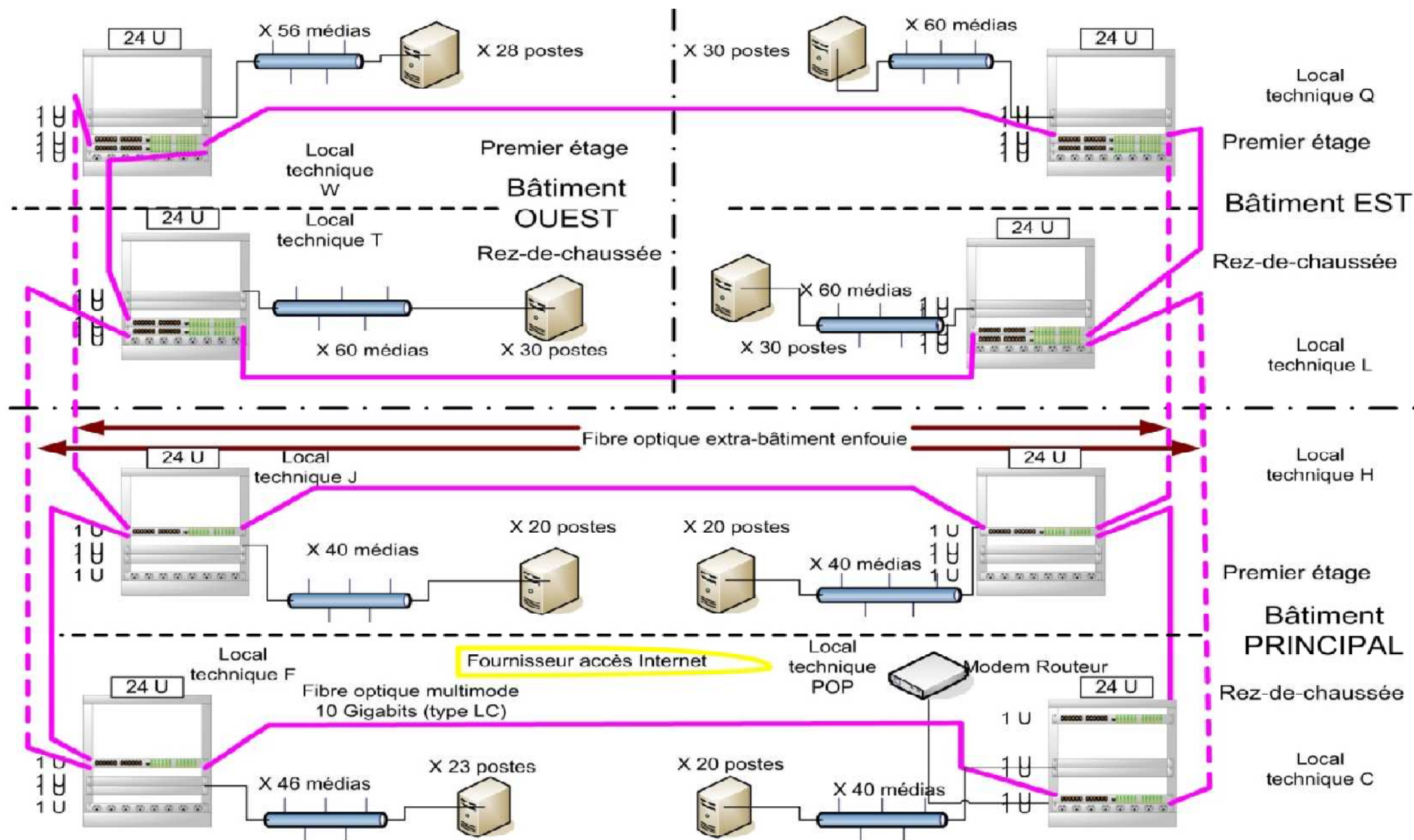
Nous aurions pu retenir le local I, qui ne nécessitait aucune modification technique.

Cependant, le local J est situé exactement au-dessus du local F, contrairement au local I qui est au centre du bâtiment.

Retenir le local J nous semble plus judicieux pour le câblage du backbone et pour la zone de couverture (rayon de 50 m). Bien que l'argument des 50 mètres ne soit pas le plus prépondérant - le bâtiment mesurant 40 m x 27 m - nous nous permettons de prévoir un futur branchement vers l'extérieur ou une meilleure répartition générale pour de futures améliorations.

Pour tout le reste de la conception du réseau, les tableaux (format microsoft excel) complète la suite de ce travail. Ils ne sont pas, de part leur dimensions, affichable en format MS word; Simplement pour ne pas nuire à leur compréhension.

le logiciel Visio nous a permis de réaliser le plan de câblage général.

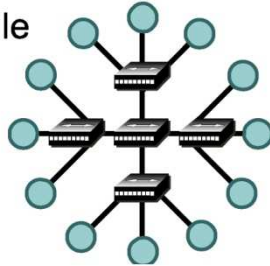


7. Topologie logique

3.3 Topologie du réseau :

La topologie en étoile étendue est la plus appropriée à ce cas de figure car elle relie des étoiles individuelles en connectant les concentrateurs ou les commutateurs et permet donc d'étendre la portée et la couverture du réseau.

Topologie en étoile étendue



Nous détaillons plus amplement par la suite cette topologie et son architecture, par la suite, notamment par le biais du matériel choisi.

8. Topologie physique

3.4 Type de câblage :

Type précis de câblage utilisé détaillé en annexes (désignation, quantité, coût).

Longueur de câblage :

Fibre optique : sachant que la distance entre le bâtiment principal et l'aile Est est de 20m et qu'elle est de 17m entre ce même bâtiment et l'aile Ouest, nous proposons la longueur de câble suivante :

- Bâtiment principal et aile Est : $20 \times 2 = 40\text{m}$
- Bâtiment principal et aile Ouest : $17 \times 2 = 34\text{m}$
- Aile Est et Aile Ouest : $20 \times 2 = 40\text{m}$
- A l'intérieur du bâtiment principal : $(40 \times 2) + 10$ (entre les étages) = 90m
- Entre les étages de l'aile Est et de l'aile Ouest : $5 \times 2 = 10\text{m}$

Soit au total : 234m

On rajoute à ce total environ 20% pour ne pas être trop juste et on obtient alors une longueur de 280m.

3.1.3 Câblage horizontal :

Il est nécessaire de respecter la norme TIA/EIA-568-A qui stipule que chaque équipement faisant partie du réseau doit être relié au concentrateur par le biais d'un câble horizontal.

3.1.4 Câblage vertical :

Il est nécessaire d'utiliser un câblage par fibre optique.

Pour les liaisons entre bâtiments, la norme sera IEEE 802.3ae 10GBASE-SR, avec des fibres de type multimode.

Pour les liaisons intra-bâtiment entre les étages et entre les

baies de brassages de respecter la norme IEEE 802.3ae 10GBASE-SR0 correspondant au câblage du backbone. Le type de média est donc en fibre optique.

3.1.5 Détails des éléments :

MATERIEL	Références	Prix unitaire TTC	Quantité ou mètre	Total (€)
Baies de brassage 19 pouces SOCAMONT 24U	43500625	564,03 €	8	4 512,24 €
Switch 48 ports	GSM7352S	3 690,00 €	8	29 520,00 €
Switch 24 ports	GSM7328S	2 449,00 €	4	9 796,00 €
Kit de Stack 24Gbit avec 2 Modules + cordon	AX742	443,00 €	4	1 772,00 €
Module adaptateur 10Gbit Ethernet XFP	AX741	776,00 €	24	18 624,00 €
Transceiver XFP Fibre 10Gbit Ethernet LC multimode	AXM751	2 290,00 €	24	54 960,00 €
Modem Routeur Firewall VPN 50 tunnels	DGFV338	349,00 €	1	349,00 €
Onduleurs		200,00 €	8	1 600,00 €
Prise para-foudre 8 blocs		40,00 €	8	320,00 €
Fibre optique multimode	10GBASE-SR	2,00 €	280	560,00 €
Cable SF/UTP cat. 6 (mur / baie de brassage) (une gaine 4 medias)	1000BASE-T	1,00 €	3400	3 400,00 €
Cordon de brassage RJ45 , bleu, S/FTP, CAT6, GigaTrue® 250 MHz avec connecteurs surmoulés, 3 m (liaisons Switch / panneaux de brassage)	EVE631-0010	12,40 €	480	5 952,00 €
Cable S/FTP cat. 6 RJ45 5m (utilisateurs / mur)		8,36 €	408	3 410,88 €
Divers petit matériel non prévus		500,00 €	1	500,00 €
Matériel du personnel				
Ordinateur portable		800,00 €	3	2 400,00 €
Connectique et ensemble complet d'outils de travail		250,00 €	3	750,00 €

Matériel de rechange				
2 switch 48 ports	GSM7352S	3 690,00 €	2	7 380,00 €
2 Transceiver XFP Fibre 10 Bit Ethernet LC multimode	AXM751	2 290,00 €	2	4 580,00 €
1 Modem Routeur Firewall VPN 50 Tunnels	DGFV338	349,00 €	1	349,00 €
Kit de Stack 24Gbit avec 2 Modules + cordon	AX742	443,00 €	1	443,00 €
Cable F/UTP cat. 6 RJ45 5m (utilisateurs / mur)		8,36 €	10	83,60 €
Cordon de brassage RJ45 , bleu, S/FTP, CAT6, GigaTrue® 250 MHz avec connecteurs surmoulés, 3 m (liaisons Switch / panneaux de brassage)	EVE631-0010	12,40 €	10	124,00 €
TOTAL		18 603,52 €	4 682	146 873,48 €

Normes des cables RJ45

Type de câble		Blindage du câble	Blindage des paires torsadées
Ancienne appellation	Nouvelle appellation		
SSTP	S/FTP	S: écran constitué d'une tresse	F: écran formé d'un ruban alu/polyester
SFTP	SF/UTP	SF: association ruban + tresse	U: aucun écran
STP	U/FTP	U: Aucun écran	F: écran formé d'un ruban alu/polyester
FTP	F/UTP	F: Écran formé d'un ruban alu/polyester	U: aucun écran
UTP	U/UTP	U: Aucun écran	U: aucun écran

9. **Matrices de résolution de problèmes**

Mode dégradé abordé à l'oral lors de la présentation.

Nous avons prévu un câblage général suffisant en cas de pannes conséquentes.

Du matériel a été prévu en remplacement. (Cf. tableau précédent)

Non créé

10. **Récapitulatif des prises et des câbles,**

Cf. dossier en format EXCEL :

Etudes de cas 1 - conception réseaux informatique.xlsx

Onglet : Référence matérielle

11. **Récapitulatif des équipements de réseau, des adresses MAC et des adresses IP.**

Cf. dossier en format EXCEL :

Etudes de cas 1 - conception réseaux informatique.xlsx

Onglet : Locaux + Salles + IP

		Référencement des locaux																								Total (horizontaux)			
		Batiment principal												Batiment EST						Batiment OUEST						3			
		Rez-de-Chaussée								Premier étage				R.-de-C.		1 ^{er} étage		R.-de-C.		1 ^{er} étage		6							
Appellation des locaux		A	B	C	D	E	F		NR	POP	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	25	
CONTRAINTES																													
Nombre des prises		250 V / 50 Hz	0	2	4	4	3	4			4	5	6	2	1	3	2	4	4	4	4	4	3	4	4	4	2	77	
Eclairage	fluorescent	oui	oui									oui		oui			oui			oui					oui			7	0
	incandescent			oui	oui	oui	oui				oui		oui		oui	oui		oui	oui		oui	oui	oui	oui		oui	oui	16	0
Interrupteur intérieur	a gauche		oui								oui				oui	oui	oui		oui	oui	oui	oui		oui	oui			11	0
	a droite	oui		oui	oui	oui	oui					oui	oui				oui					oui			oui	oui		11	0
Interrupteur extérieur														oui									oui			oui	oui	1	0
Porte	ouverture intérieure	oui	oui								oui			oui														4	0
	ouverture extérieure			oui	oui	oui	oui					oui	oui	oui		oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	19	0
Serrure	"présence"	non	oui	oui	oui	oui	oui				oui	oui	oui	non	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	21	2
plafond	suspendu	oui	oui	non	non	non	non				oui	non	non	oui	non	non	non	non	oui		non	non	non	non	non	non	non	5	17
Murs	peinture ignifuge	oui	oui	oui	oui	oui	oui				oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui	oui			oui	21	0
	amiante																								oui	oui		2	0
Canalisation eau			oui								oui						oui		oui			oui			oui			6	0
produits chimiques toxiques														oui														1	0
Ligne principale d'alimentation en électricité					oui									oui			oui				oui							4	0
Equipement du répartiteur principal				oui					non																			1	1
Local technique secondaire							oui					oui		oui							oui			oui			oui	3	0
												oui		oui						oui						oui		4	0
Détermination des locaux techniques																										total de	total de		
rouge = normes non conformes		Vert = Normes conformes																								"oui"	"non"		

Salles	Distance (m) du câblage baies de brassage / utilisateurs						Total (m)	Multiplicateur d'échelle des plans de travail	Salles	Distance (m) du câblage baies de brassage / utilisateurs						Total (m)	
	Batiment principal		Batiment EST		Batiment OUEST					Batiment principal		Batiment EST		Batiment OUEST			
	R.-de-C.	1 ^{er} étage	R.-de-C.	1 ^{er} étage	R.-de-C.	1 ^{er} étage				R.-de-C.	1 ^{er} étage	R.-de-C.	1 ^{er} étage	R.-de-C.	1 ^{er} étage		
	Local technique C	Local technique H	Local technique L	Local technique Q	Local technique T	Local technique w		1 cm sur plan vaut X m réels		Local technique C	Local technique H	Local technique L	Local technique Q	Local technique T	Local technique w		
	Local technique F	Local technique J						Bat. Principal	2,55		Local technique F	Local technique J					
101	10		12		12		34	Bat. Est	2,16	101	25,48	0,00	25,95	0,00	25,95	0,00	77,37
102	10		12		12		34	Bati. Ouest	2,16	102	25,48	0,00	25,95	0,00	25,95	0,00	77,37
103	10		12		12		34			103	25,48	0,00	25,95	0,00	25,95	0,00	77,37
104	1		12		12		25			104	2,55	0,00	25,95	0,00	25,95	0,00	54,44
105	10		12		12		34			105	25,48	0,00	25,95	0,00	25,95	0,00	77,37
106	10		17		17		44			106	25,48	0,00	36,76	0,00	36,76	0,00	98,99
107			17		17		34			107	0,00	0,00	36,76	0,00	36,76	0,00	73,51
108	10						10			108	25,48	0,00	36,76	0,00	0,00	0,00	62,23
109 a	10		17		17		44			109 a	25,48	0,00	36,76	0,00	36,76	0,00	98,99
109 b	10						10			109 b	25,48	0,00	36,76	0,00	0,00	0,00	62,23
110	10		17		17		44			110	25,48	0,00	36,76	0,00	36,76	0,00	98,99
111	10		17		17		44			111	25,48	0,00	36,76	0,00	36,76	0,00	98,99
112	10		12		12		34			112	25,48	0,00	25,95	0,00	25,95	0,00	77,37
113	10		12		12		34			113	25,48	0,00	25,95	0,00	25,95	0,00	77,37
114	10		12		12		34			114	25,48	0,00	25,95	0,00	25,95	0,00	77,37
115	10		12		12		34			115	25,48	0,00	25,95	0,00	25,95	0,00	77,37
116	10		12		12		34			116	25,48	0,00	25,95	0,00	25,95	0,00	77,37
117	10						10			117	25,48	0,00	25,95	0,00	0,00	0,00	51,42
118	10						10			118	25,48	0,00	0,00	0,00	0,00	0,00	25,48
119	10						10			119	25,48	0,00	0,00	0,00	0,00	0,00	25,48
120	10						10			120	25,48	0,00	0,00	0,00	0,00	0,00	25,48
121	10						10			121	25,48	0,00	0,00	0,00	0,00	0,00	25,48
122	10						10			122	25,48	0,00	0,00	0,00	0,00	0,00	25,48
201		10		17			27			201	0,00	0,00	0,00	36,76	0,00	0,00	36,76
202		10		17		17	44			202	0,00	25,48	0,00	36,76	0,00	36,76	98,99
203		10		17		17	44			203	0,00	25,48	0,00	36,76	0,00	36,76	98,99
204		10		12		12	34			204	0,00	25,48	0,00	25,95	0,00	25,95	77,37
205		10		12		12	34			205	0,00	25,48	0,00	25,95	0,00	25,95	77,37
206		10		12		12	34			206	0,00	25,48	0,00	25,95	0,00	25,95	77,37
207	10	10		12		12	44			207	25,48	25,48	0,00	25,95	0,00	25,95	102,85
208		10		12		12	34			208	0,00	25,48	0,00	25,95	0,00	25,95	77,37
209		10		12		12	34			209	0,00	25,48	0,00	25,95	0,00	25,95	77,37
210				12		12	24			210	0,00		0,00	25,95	0,00	25,95	51,89
211				12		12	24			211	0,00		0,00	25,95	0,00	25,95	51,89
212		10		12		12	34			212	0,00	0,00	0,00	25,95	0,00	25,95	51,89
213		10		17		17	44			213	0,00	0,00	0,00	36,76	0,00	36,76	73,51
214		10		17		17	44			214	0,00	25,48	0,00	36,76	0,00	36,76	98,99
215		10		17		17	44			215	0,00	25,48	0,00	36,76	0,00	36,76	98,99
216		10					10			216	0,00	25,48	0,00	0,00	0,00	0,00	25,48
217		10					10			217	0,00	25,48	0,00	0,00	0,00	0,00	25,48
218		10					10			218	0,00	25,48	0,00	0,00	0,00	0,00	25,48
219		10					10			219	0,00	25,48	0,00	0,00	0,00	0,00	25,48
220		10					10			220	0,00	25,48	0,00	0,00	0,00	0,00	25,48
221		10					10			221	0,00	25,48	0,00	0,00	0,00	0,00	25,48
TOTAL (m)							1224	TOTAL (m)							2828,00		
% d'ajustement							20,00%	% d'ajustement							20,00%		
TOTAL (m)							1468,8	TOTAL (m)							3393,60		

221	190	205	210	205	193	Total
265,2	228	246	210	205	193	Total + ajustement

563,06	407,64	542,70	454,05	443,24	417,30	Total
675,67	489,17	651,24	454,05	443,24	417,30	Total + ajustement

44	23	19	15	15	15	14	Vérification nombre de salles connectées
----	----	----	----	----	----	----	---

Référencement des locaux	Nombre de postes de travail initiaux prévus par salle						Adressage des medias destinés aux postes de travail initiaux prévus par salle					
	Batiment principal		Batiment EST		Batiment OUEST		Batiment principal		Batiment EST		Batiment OUEST	
	Rez-de-Chaussée	Premier étage	R.-de-C.	1 ^{er} étage	R.-de-C.	1 ^{er} étage	Rez-de-Chaussée	1 ^{er} étage	R.-de-C.	1 ^{er} étage	R.-de-C.	1 ^{er} étage
par étage	46	40	30	30	30	28	92	80	60	60	60	56
par batiment	86		60		58		172		120		116	
de l'infrastructure	204						408					
Salle N° 101	2		2		2		172.16.0.1		172.16.2.1		172.16.4.1	
							172.16.0.2		172.16.2.2		172.16.4.2	
							172.16.0.3		172.16.2.3		172.16.4.3	
							172.16.0.4		172.16.2.4		172.16.4.4	
Salle N° 102	2		2		2		172.16.0.5		172.16.2.5		172.16.4.5	
							172.16.0.6		172.16.2.6		172.16.4.6	
							172.16.0.7		172.16.2.7		172.16.4.7	
							172.16.0.8		172.16.2.8		172.16.4.8	
Salle N° 103	2		2		2		172.16.0.9		172.16.2.9		172.16.4.9	
							172.16.0.10		172.16.2.10		172.16.4.10	
							172.16.0.11		172.16.2.11		172.16.4.11	
							172.16.0.12		172.16.2.12		172.16.4.12	
Salle N° 104	2		2		2		172.16.0.13		172.16.2.13		172.16.4.13	
							172.16.0.14		172.16.2.14		172.16.4.14	
							172.16.0.15		172.16.2.15		172.16.4.15	
							172.16.0.16		172.16.2.16		172.16.4.16	
Salle N° 105	2		2		2		172.16.0.17		172.16.2.17		172.16.4.17	
							172.16.0.18		172.16.2.18		172.16.4.18	
							172.16.0.19		172.16.2.19		172.16.4.19	
							172.16.0.20		172.16.2.20		172.16.4.20	
Salle N° 106	2		2		2		172.16.0.21		172.16.2.21		172.16.4.21	
							172.16.0.22		172.16.2.22		172.16.4.22	
							172.16.0.23		172.16.2.23		172.16.4.23	
							172.16.0.24		172.16.2.24		172.16.4.24	
Salle N° 107			2		2				172.16.2.25		172.16.4.25	
									172.16.2.26		172.16.4.26	
									172.16.2.27		172.16.4.27	
									172.16.2.28		172.16.4.28	
Salle N° 108	2						172.16.0.29					
							172.16.0.30					
							172.16.0.31					
							172.16.0.32					
Salle N° 109 a	2		2		2		172.16.0.33		172.16.2.33		172.16.4.33	
							172.16.0.34		172.16.2.34		172.16.4.34	
							172.16.0.35		172.16.2.35		172.16.4.35	
							172.16.0.36		172.16.2.36		172.16.4.36	
Salle N° 109 b	2						172.16.0.37					
							172.16.0.38					
							172.16.0.39					
							172.16.0.40					
Salle N° 110	2		2		2		172.16.0.41		172.16.2.41		172.16.4.41	
							172.16.0.42		172.16.2.42		172.16.4.42	
							172.16.0.43		172.16.2.43		172.16.4.43	
							172.16.0.44		172.16.2.44		172.16.4.44	
Salle N° 111	2		2		2		172.16.0.45		172.16.2.45		172.16.4.45	
							172.16.0.46		172.16.2.46		172.16.4.46	
							172.16.0.47		172.16.2.47		172.16.4.47	
							172.16.0.48		172.16.2.48		172.16.4.48	
Salle N° 112	2		2		2		172.16.0.49		172.16.2.49		172.16.4.49	
							172.16.0.50		172.16.2.50		172.16.4.50	
							172.16.0.51		172.16.2.51		172.16.4.51	
							172.16.0.52		172.16.2.52		172.16.4.52	
Salle N° 113	2		2		2		172.16.0.53		172.16.2.53		172.16.4.53	
							172.16.0.54		172.16.2.54		172.16.4.54	
							172.16.0.55		172.16.2.55		172.16.4.55	
							172.16.0.56		172.16.2.56		172.16.4.56	
Salle N° 114	2		2		2		172.16.0.57		172.16.2.57		172.16.4.57	
							172.16.0.58		172.16.2.58		172.16.4.58	
							172.16.0.59		172.16.2.59		172.16.4.59	
							172.16.0.60		172.16.2.60		172.16.4.60	
Salle N° 115	2		2		2		172.16.0.61		172.16.2.61		172.16.4.61	
							172.16.0.62		172.16.2.62		172.16.4.62	
							172.16.0.63		172.16.2.63		172.16.4.63	
							172.16.0.64		172.16.2.64		172.16.4.64	
Salle N° 116	2		2		2		172.16.0.65		172.16.2.65		172.16.4.65	
							172.16.0.66		172.16.2.66		172.16.4.66	
							172.16.0.67		172.16.2.67		172.16.4.67	
							172.16.0.68		172.16.2.68		172.16.4.68	
Salle N° 117	2						172.16.0.69					
							172.16.0.70					
							172.16.0.71					
							172.16.0.72					
Salle N° 118	2						172.16.0.73					
							172.16.0.74					
							172.16.0.75					
							172.16.0.76					

ANNEXE 2

**Mise à jour personnelle du local
technique AFPA, bâtiment 14.
(Extrait)**

BAIE DE BRASSAGE

prise murale / panneau	Device 1	Connect°	Adressage IP	Device 2	Salle	Personnes
1A01					Etage 1 - Salle 5	
1A02	Switch C	1		Serveur Dell 500	Etage 1 - Salle 5	Formateurs
1A03	Switch C	2		Transtec	Etage 1 - Salle 5	Formateurs
1A04					Etage 1 - Salle 5	
1A05					Etage 1 - Salle 5	
1A06	Switch C	3		Photocopieuse	Etage 1 - Salle 5	Formateurs
1A07					Etage 1 - Salle 6	
1A08					Etage 1 - Salle 6	
1A09					Etage 1 - Salle 6	
1A10	Switch C	4		Salle d'entretien	Etage 1 - Salle 6	Formateurs
1A11					Etage 1 - Salle 4	
1A12	Panneau C	7		Téléphone formateur	Etage 1 - Salle 4	Formateurs
1A13	Switch C	5		PC AFPA	Etage 1 - Salle 4	M P. Quarrey
1A14	Switch C	6		PC AFPA portable	Etage 1 - Salle 4	M P. Quarrey
1A15	Panneau C	7		Prise téléphone RJ11	Etage 1 - Salle 4	Formateurs
1A16	Switch C	7		PC AFPA portable	Etage 1 - Salle 4	M Y. kohler
1A17	Switch A	1		PC AFPA	Etage 1 - Salle 3	Marc & Ludo
1A18	Switch A	2		Imprimante RICOH	Etage 1 - Salle 3	Formateurs
1A19	Switch A	3		PC AFPA	Etage 1 - Salle 3	Cédric
1A20	Switch A	4		PC AFPA	Etage 1 - Salle 3	Gauthier
1A21	Switch A	14		PC AFPA	Etage 1 - Salle 3	Serveur Peda
1A22	Switch A	5		PC AFPA	Etage 1 - Salle 3	Olivier
1A23	Switch A	6		Routeur wifi	Etage 1 - Salle 3	Michaël
1A24	Switch A	7		PC portable	Etage 1 - Salle 3	Michaël
1A25	Switch A	8		PC AFPA	Etage 1 - Salle 3	Eric
1A26	Switch A	9		PC portable	Etage 1 - Salle 3	Arnaud
1A27	Switch A	10		PC AFPA	Etage 1 - Salle 3	Serveur Linux
1A28	Switch A	11		PC AFPA	Etage 1 - Salle 3	Simon
1A29					Etage 1 - Salle 3	
1A30	Switch A	12		PC AFPA	Etage 1 - Salle 3	Arnaud
1A31	Switch A	13		PC AFPA	Etage 1 - Salle 3	Vladimir

1B23	Switch B	12		PC AFPA	Etage 1 - Salle 1	Michaël
1B24	Switch B	13		PC AFPA	Etage 1 - Salle 1	Francis
1B25					Etage 1 - Salle 1	
1B26					Etage 1 - Salle 1	
1B27	Switch B	14		PC AFPA	Etage 1 - Salle 1	Amélie
1B28	Switch B	15		PC portable	Etage 1 - Salle 1	Amélie
1B29	Switch B	16		PC AFPA	Etage 1 - Salle 1	Mike
1B30	Switch B	22		PC portable	Etage 1 - Salle 1	Mike
1B31	Switch B	17		PC AFPA	Etage 1 - Salle 1	Eman P.
1B32	Switch B	18		PC portable	Etage 1 - Salle 1	Eman P.
1B33	Switch B	19		PC AFPA	Etage 1 - Salle 1	Olivier
1B34	Switch B	20		PC portable	Etage 1 - Salle 1	Olivier
1B35					Etage 1 - Salle 1	
1B36					Etage 1 - Salle 1	
1B37					Etage 1 - Salle 1	
1B38					Etage 1 - Salle 1	
1B39					Etage 1 - Salle 1	
1B40					Etage 1 - Salle 1	
1B41					Etage 1 - Salle 1	
1B42					Etage 1 - Salle 1	
1B43					Etage 1 - Salle 1	
1B44					Etage 1 - Salle 1	
1B45					Etage 1 - Salle 1	
1B46					Etage 1 - Salle 1	
1B47	Switch B	21		PC AFPA	Etage 1 - Salle 1	Damien
1B48	Switch C	13		Coffreur Brancheur	Etage 0 - salle 1	Formateurs
1C01	Switch C	14		PC AFPA portable	Etage 1 - Salle 1	M Y. kohler
1C02						
1C03						
1C04						
1C05						
1C06						
1C07	Panneau A	12		téléphone sur IP	Etage 1 - salle 4	Formateurs
1C08						
1C09						
1C10						
1C11						
1C12						
1C13	Modem	1		modem général	Etage 1 - salle 5	Formateurs

ANNEXE 3

**Amélioration et synthèse d'une
procédure pour récupérer la
configuration IOS d'un routeur**

Procédure pour récupérer la configuration IOS d'un routeur

Ce cas arrive s'il y a eu conjointement :

- erase flash
- erase running-config

Matériel nécessaire : 1 ordinateur, 2 routeurs : 1 routeur sans IOS et 1 routeur avec IOS

RECUPERATION :

0) changer les propriétés de la carte réseau qui sera reliée au routeur

exemple : adresse IP = 192.168.4.5
 masque adresse = 255.255.255.0
 passerelle = 192.168.4.1

1) Installer sur l'ordinateur un serveur TFTP

ex : TFTP32

configurer serveur TFTP

current Directory = le répertoire où l'image sera sauvegardé

serveur Interface = l'interface de l'ordinateur (car c'est le pc qui fait serveur !)

= adresse ip statique pour la carte réseaux du PC (reliée au routeur)
(192.168.4.5)

1-1) Connaître l'adresse IP du PC

2) Relier le routeur avec l'IOS correcte au PC par un câble croisé

Choisir le port FastEthernet 0/0 ou Fast ethernet 0/1

Allumer le routeur

3) Ouvrir le programme HyperTerminal

Effectuer les commandes suivantes

Attendre le chargement de la configuration

si besoin ensuite "entrer le mot de passe du routeur"

"enable" pour passer en mode privilégié

"mot de passe mode privilégié"

dans tous les cas, passer en mode privilégié (exemple fini : router#)

Vérifier physiquement à quel FastEthernet est relié le câble croisé !

"show interface"

--> vérifier l'adresse IP pour le fast ethernet 0/0 et fast ethernet 0/1

Attention: le masque de réseaux Fast Ethernet est : 255.255.255.0

donc l'adresse ip doit être par exemple 192.168.4.xxx

"ping xxx.xxx.xxx.xxx" avec l'adresse du PC (permet de vérifier que le routeur voit le pc)
(ping 192.168.4.5)

4) Sur l'ordinateur, ouvrir une fenêtre de commande (menu démarrer, exécuter, cmd)

Faire les commandes suivantes :

"ping xxx.xxx.xxx.xxx" avec l'adresse du routeur (permet de vérifier que l'ordinateur voit le routeur) (ping 192.168.4.4)

5) Sur HyperTerminal, faire les commandes suivantes :

copy running-config flash ---> copie la configuration courante en mémoire flash (celle de la carte flash)

Show flash ---> permet de voir le nom du fichier extension .bin (noté ce nom au complet)

copy flash tftp ---> copie la mémoire flash vers le pc

À l'invite : Address or name of remote host : rentrer l'adresse IP statique mise pour le serveur TFTP sur le PC

À l'invite : Destination filename [c2800nm-ipbase-mz.124-3g.bin]? : appuyer sur entrer pour garder le même nom !
et là attendre la fin des « !!!!!!!!!!!!!!! ... »

6) Retirer sans éteindre la carte compact Flash avec l'IOS

Mettre dans le routeur sans IOS la carte compact flash avec IOS

Faire les commandes

copy tftp flash ---> copie le contenu du fichier sur le pc de la mémoire flash

À l'invite : Address or name of remote host : rentrer l'adresse IP statique mise pour sur le ROUTEUR

À l'invite : Destination filename [c2800nm-ipbase-mz.124-3g.bin]? : appuyez sur entrer pour garder le même nom !

Et là attendre de revenir à une invite en mode privilège.

6.6) Eteindre le routeur et le redémarrer

7) en cas de soucis, bien vérifier que l'adresse Fast Ethernet sur le routeur soit toujours celle défini au départ !!!

Bonne manipulation

Olivier H.

ANNEXE 4

Etude de cas CISCO, CCNA 2

Le routage

(Extrait)

CISCO

Etude de cas

CCNA 2

LE ROUTAGE

Responsable de formation :

M. Yannick KOHLER

Formateur T.S.R.I.T.E.

A.F.P.A. Besançon



gagnez en **compétences**

Stagiaire :

M. Olivier HOUBLOUP

(E-m@il : Olivier.afpa@yahoo.fr)

Année 2008-2009

Remerciements

Je tiens à remercier toutes les personnes qui ont participé à la bonne réussite de cette étude de cas.

A mon formateur, M. Yannick KOHLER pour sa patience face à mes questions. J'aurais mérité quelques fois de réfléchir d'avantage avant de demander la réponse.

A mon collègue, M. Emmanuel POIRRIER pour son aide méthodologique et sa pédagogie lorsque je ne trouvais pas les bons axes de réflexion.

Sommaire :

Remerciements :	1
Sujet :	3
Introduction :	17
<i>PHASE 1 : Description du projet :</i>	18
<i>PHASE 2 : Adressage IP :</i>	21
<i>PHASE 3 : Configuration de base des routeurs et des stations de travail :</i>	25
<i>PHASE 4 : Listes de contrôle d'accès :</i>	29
<i>PHASE 5 : Documentation du réseau :</i>	31
<i>Conclusion et réflexion :</i>	36
Annexes :	38
Compilation des vidéos	
Comparaisons des protocoles de routage	
Le protocole OSPF	
Adressage IP et configuration des routeurs	
Commentaires des vidéos	

N.B. : Tous les mots suivis d'un astérisque (*) sont répertoriés dans le glossaire.

Le routage

Programme Cisco Networking Academy Program

CCNA 2: Notions de base sur les routeurs et le routage (version 3.1)

+ Corrections pages 4 - 7 - 9

Vue d'ensemble et objectifs

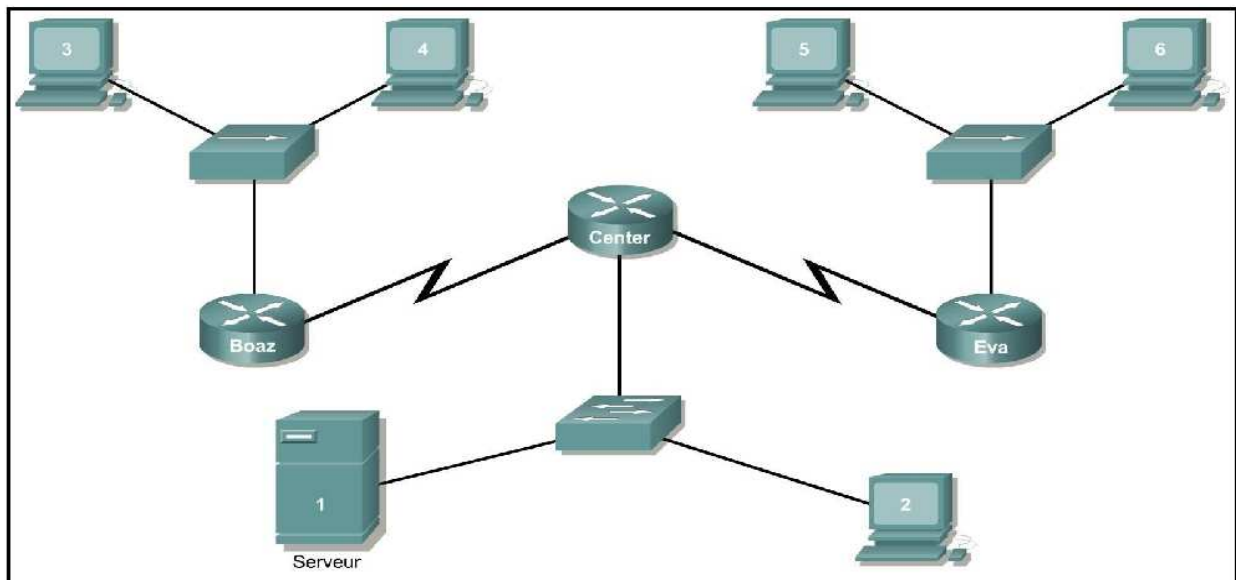
Cette étude cas permet aux étudiants de réaliser un projet de conception, de mise en oeuvre et de dépannage de projets en utilisant les compétences acquises au cours du programme CCNA 2. Ils utiliseront ensuite ces compétences pour utiliser, fabriquer et connecter le câblage adéquat aux unités appropriées.

Il est crucial de lire et de comprendre les scénarios afin de s'assurer que toutes les exigences sont satisfaites. Chaque scénario guide l'étudiant à travers les étapes appropriées en vue d'une exécution complète du projet.

Au cours de cette étude de cas, l'étudiant doit accomplir les étapes suivantes :

- Mettre en place la configuration physique du réseau en utilisant le schéma et l'exposé oral qui l'accompagne
- Configurer correctement les routeurs avec une configuration de routeur de base
- Configurer un serveur TFTP sur l'une des stations de travail
- Créer et appliquer des listes de contrôle d'accès sur le ou les routeur(s) et les interface(s)
- Dépanner et tester l'ensemble de la connectivité et des listes de contrôle d'accès
- Soumettre une documentation détaillée sous la forme prescrite, conformément à la liste de la section sur les travaux demandés

Scénario et Phase 1 : Description du projet



Au sein d'une société, plusieurs personnes sont responsables de la maintenance de diverses sections de l'infrastructure d'interréseau. Beaucoup de techniciens ont fait un excellent travail pour ce qui concerne la petite partie dont ils sont responsables.

L'un des associés réseau responsable d'une grande partie de l'infrastructure a soudainement quitté la société. La reconception et la mise en oeuvre de cette portion de l'interréseau est de ce fait incomplète. Il est donc confié à un technicien la mission de terminer le travail.

Ayant emporté la documentation chez lui pour la lire durant le week-end, le technicien comprend pourquoi l'associé réseau a préféré abandonner sa tâche. Les quelques documents qui existent sont mal écrits. Pendant le week-end, le technicien reconstruit le schéma ci-dessus en se basant sur un schéma existant. Il représente la nouvelle conception de l'interréseau. Il montre les routeurs, les concentrateurs/commutateurs, les circuits et les serveurs/stations de travail qui sont prévus sur chaque site. Le serveur du site Center est un serveur de fichiers auxquels seules les stations de travail de cet interréseau peuvent accéder. La station de travail du site Center est utilisée pour gérer tous les routeurs sur l'interréseau.

Le lundi matin, le technicien présente le nouveau schéma au chef d'équipe Infrastructure réseau qui lui a confié le projet. Après discussion, il est décidé qu'une nouvelle documentation doit être développée pour le projet. Le chef d'équipe et le professeur doivent approuver la documentation à chaque phase du processus. Utilisez les informations suivantes pour mettre en oeuvre le réseau.

Adresse réseau _____

Nombre de sous-réseaux nécessaires _____

Protocole de routage _____

Phase 2 : Adressage IP

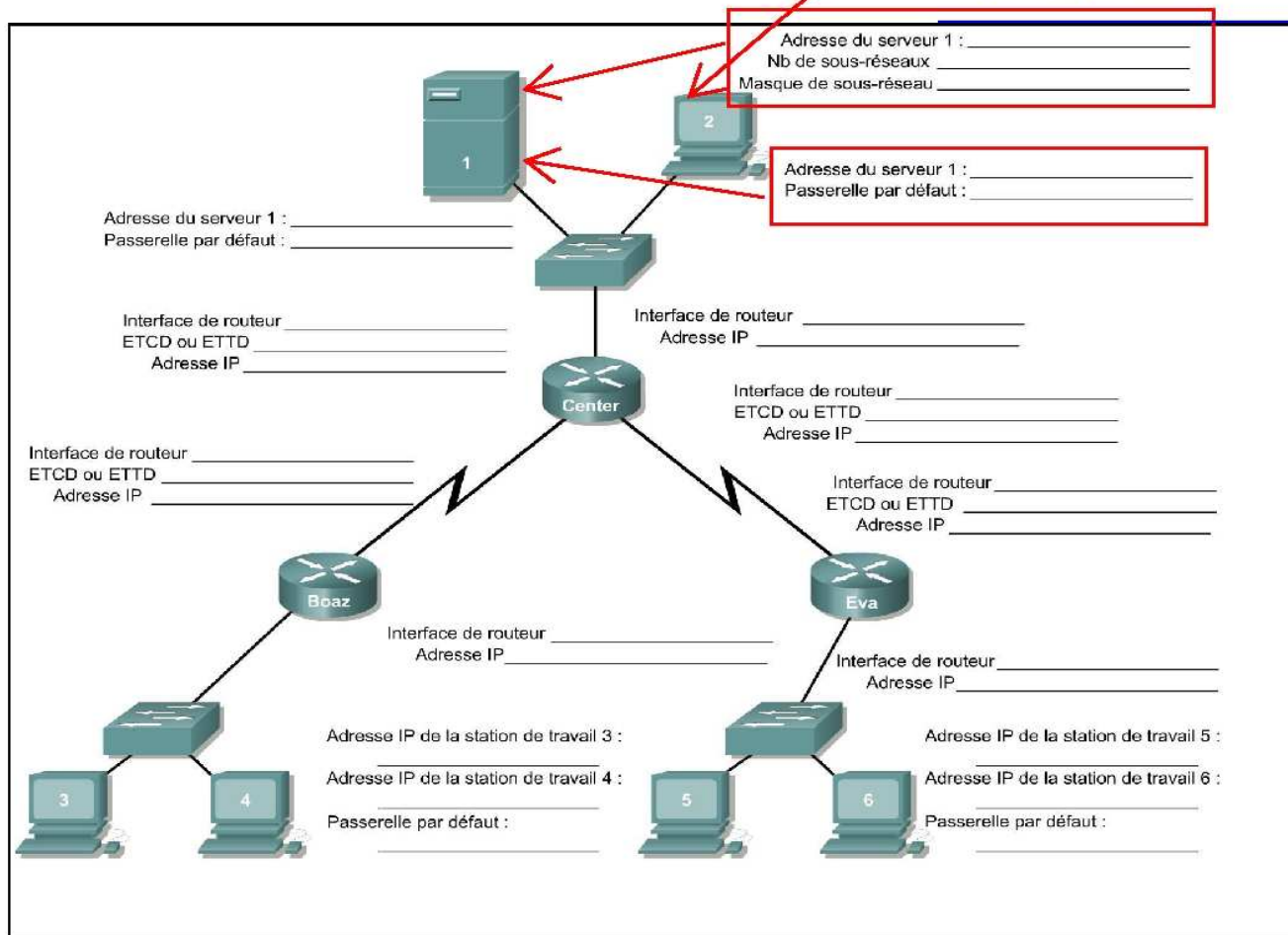
Maintenant que le plan de base est en place, le chef d'équipe demande au technicien de développer un prototype pour le nouvel interrèseau. Utilisez l'adresse réseau attribuée ainsi que les exigences propres aux sous-réseaux, afin d'établir le sous-réseau du réseau. À partir du système d'adressage IP, attribuez des adresses IP aux interfaces appropriées sur tous les routeurs et ordinateurs de l'interrèseau. Utilisez le schéma ci-dessous comme guide. Avant de passer à la Phase 3, vous devez obtenir l'approbation de cette phase de développement auprès du chef d'équipe.

Accord du professeur _____ Date _____

Station de travail 2
IP de la la station de travail2 :

Passerelle par défaut :

Schéma du réseau – Adressage IP



Phase 3 : Configuration de base des routeurs et des stations de travail

Après avoir inspecté le câblage du prototype, le chef d'équipe demande au technicien de créer une configuration de base pour le routeur et les stations de travail.

Utilisez le schéma et les fiches de planification pour créer une configuration de base pour le routeur. La liste de contrôle ci-dessous vous aidera à suivre le processus de configuration.

	Boaz	Center	Eva
Nom d'hôte			
Mot de passe de console			
Mot de passe « enable secret »			
Mot de passe VTY			
Adresse IP Serial 0/0			
Adresse IP Serial 0/1			
*Fréquence d'horloge Serial 0/0			
*Fréquence d'horloge Serial 0/1			
Adresse IP Fa 0/0			
Adresse IP Fa 0/1			
Activer les interfaces			
Ajouter un protocole de routage			
Ajouter des instructions réseau			

Remarque * : Selon le besoin

Suite du tableau sur la page suivante

	Boaz	Center	Eva
* Table d'hôtes - contient tous les routeurs et serveurs			
Message du jour			
Description Serial 0/0			
Description Serial 0/1			
Description Fa 0/0			
Description Fa 0/1			

Accord du professeur _____ Date _____

Phase 4 : Listes de contrôle d'accès

Lors du test du réseau, le chef d'équipe découvre que la sécurité n'a pas été planifiée. Si la configuration du réseau était installée telle quelle, n'importe quel utilisateur du réseau serait en mesure d'accéder à l'ensemble des unités et des postes de travail du réseau.

Le chef d'équipe demande au technicien d'ajouter des listes de contrôle d'accès (ACL) aux routeurs. Il émet certaines suggestions pour développer la sécurité. Avant d'ajouter les listes de contrôle d'accès, sauvegardez la configuration de routeur actuelle. Assurez-vous également de la connectivité totale au sein du réseau avant d'appliquer une quelconque liste de contrôle d'accès.

Les conditions suivantes doivent être prises en compte lors de la création des listes de contrôle d'accès :

- La station de travail 2 et le serveur de fichiers 1 se trouvent sur le réseau de gestion. N'importe quelle unité du réseau de gestion peut accéder à n'importe quel équipement sur l'ensemble du réseau.
- Les stations de travail connectées aux LAN Eva et Boaz ne sont pas autorisées en dehors de leur sous-réseau, sauf pour accéder au serveur de fichiers 1.
- Chaque routeur peut envoyer une requête telnet aux autres routeurs et accéder à n'importe quelle unité sur le réseau.

Le chef d'équipe demande au technicien de rédiger un bref résumé du rôle de chaque liste de contrôle d'accès, des interfaces sur lesquelles elles seront appliquées et de la direction du trafic. Dressez ensuite la liste exacte des commandes qui seront utilisées pour créer et appliquer les listes de contrôle d'accès aux interfaces du routeur.

Avant de configurer les listes de contrôle d'accès sur les routeurs, passez en revue chacune des conditions de test suivantes et vérifiez que les listes de contrôle d'accès vont se comporter comme prévu :

Connexion TELNET de Boaz à Eva	RÉUSSIE
Connexion TELNET de la station de travail 4 à Eva	BLOQUÉE
Connexion TELNET de la station de travail 5 à Boaz	BLOQUÉE
Connexion TELNET de la station de travail 2 à Boaz	RÉUSSIE
Connexion TELNET de la station de travail 2 à ~~Boaz~~ Eva	RÉUSSIE
Requête ping de la station de travail 5 vers le serveur de fichiers 1	RÉUSSIE
Requête ping de la station de travail 3 vers le serveur de fichiers 1	RÉUSSIE
Requête ping de la station de travail 3 vers la station de travail 4	RÉUSSIE
Requête ping de la station de travail 3 vers la station de travail 6	RÉUSSIE
Requête ping de la station de travail 3 vers la station de travail 5	BLOQUÉE

Requête ping de la station de travail 2 vers la station de travail 5	RÉUSSIE
Requête ping de la station de travail 2 vers la station de travail 3	RÉUSSIE
Requête ping du routeur Eva vers la station de travail 3	RÉUSSIE
Requête ping du routeur Boaz vers la station de travail 5	RÉUSSIE

Phase 5: Documentation du réseau

La documentation est indispensable pour pouvoir assurer une prise en charge correcte du réseau. Créez une documentation qui soit organisée de façon logique pour faciliter la résolution des problèmes.

Documentation de la gestion de la configuration

	Boaz	Center	Eva
show cdp neighbors			
show ip route			
show ip protocols			
show ip interface brief			
show version			
show hosts			
show startup-config			

Documentation de la gestion de la sécurité

	Boaz	Center	Eva
show ip interface			
show ip access-lists			

Accord du professeur _____ Date _____

Travaux livrables de l'étude de cas

Le principal enseignement que l'on peut retirer de cette étude de cas est l'importance d'une documentation approfondie et claire. Deux types de documentation doivent être élaborés.

Documentation générale :

- Un exposé complet du projet doit être tapé à l'aide d'un logiciel de traitement de texte. Puisque les scénarios décomposent l'ensemble du travail en divers éléments, prenez soin de traiter chaque tâche du scénario pour que toute personne non initiée puisse comprendre cette tâche particulière.
- Microsoft Excel ou un autre programme de tableur peut être utilisé pour répertorier les équipements et les numéros de série.
- Cisco Network Designer (CND), Microsoft Visio ou tout programme de dessin peut être utilisé pour dessiner le réseau.
- Fournissez une documentation qui précise comment la sécurité a été testée. Un plan de surveillance du réseau doit également être inclus.

Documentation technique :

La documentation technique doit inclure des détails de la topologie réseau. Utilisez CND, Visio ou n'importe quel programme de dessin pour dessiner le réseau.

Utilisez les tableaux de la copie de travail de l'étude de cas comme référence, et entrez toutes les informations de ces tableaux dans un programme de tableur tel que Microsoft Excel. La feuille de calcul doit comprendre les détails suivants :

- Adressage IP de toutes les interfaces
- Informations ETCD/ETTD
- Mots de passe de routeur
- Descriptions d'interface
- Adressage IP et affectations de passerelle pour tous les PC

Les listes de contrôle d'accès proprement dites ou les séquences de commandes de routeur, doivent être incluses dans cette documentation en utilisant un programme de traitement de texte. N'oubliez pas d'inclure l'interface de routeur à laquelle la liste est appliquée ainsi que la direction.

Documentez l'utilisation d'un protocole de routage.

Le résultat sur le routeur des commandes suivantes doit être capturé et placé dans cette documentation :

- `show cdp neighbors`
- `show ip route`
- `show ip protocols`
- `show ip interface`

- `show version`
- `show hosts`
- `show startup-config`
- `show ip access-list`

Notes au professeur

Phase 1 : Description du projet

Cette phase de l'étude de cas peut être introduite au début du module, étant donné que les étudiants doivent connaître les sous-réseaux.

L'étude de cas tout entière doit être traitée en cours afin que tous les étudiants comprennent que cette étude n'a pas pour seul but la pratique de la configuration et du dépannage, mais qu'elle porte aussi sur la documentation de leur travail. Voici les références de quelques sites Web intéressants qui aideront les étudiants à comprendre la documentation :

<http://www.ittoolkit.com/articles/tech/importofdocs.htm>

<http://www.serverwatch.com/tutorials/article.php/1475021>

http://www.ethermanage.com/ethernet/100quickref/ch14qr_16.html

<http://tampabay.bizjournals.com/tampabay/stories/1997/11/24/smallb2.html>

L'adresse réseau attribuer doit appartenir à l'une des plages d'adresses IP privées ou à un sous-réseau de :

Classe	Plage
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Le protocole de routage doit être l'IGRP. La première partie de la Phase 1 devra certainement être réalisée en cours pour que les étudiants comprennent mieux l'objectif de l'étude de cas. Le travail livrable doit être traité en même temps que la description de la Phase 1. Le professeur doit déterminer s'il s'agit ou non d'un projet de groupe. Chaque étudiant doit être à même de déterminer les adresses IP des interfaces une fois le système d'adressage IP choisi.

Le Schéma du réseau – Adressage IP de la page 4 est le premier document qui doit être approuvé par le professeur.

Phase 2 : Adressage IP

Cette phase de l'étude de cas doit être soumise une fois le module 4 ou 5 terminé.

Les étudiants doivent recréer le dessin au cours de cette Phase en utilisant CDN, Visio ou un programme de dessin. Dans le dessin, les étudiants devront insérer les connexions d'interface appropriées sur les routeurs. Ce dessin doit être approuvé par le professeur.

Les sujets suivants peuvent être abordés lors des discussions en classe :

- Les raisons de l'utilisation de l'adressage IP privé

- Le concept d'espace d'adresses réservées pour les routeurs, les serveurs et les hôtes
- Les raisons du développement d'un système d'adressage IP en vue d'une croissance future

Phase 3 : Configuration de base des routeurs et des stations de travail

Cette phase doit être réalisée lorsque les étudiants se sentent à l'aise avec la configuration de base des routeurs, quelques temps après le Module 7.

Les étudiants doivent posséder quelques notions de la configuration de routeur et comprendre les exigences de base. La liste de contrôle incluse dans la Phase 3 les aidera à inclure les éléments essentiels pour la configuration de routeur. L'étudiant doit choisir la station de travail qui sera le serveur TFTP. Il doit savoir quelles sont les unités qui doivent accéder au serveur TFTP. Les étudiants doivent être guidés pour compléter le tableau de la Phase 3, et ils doivent faire approuver la configuration par le professeur.

Après l'accord du professeur, les étudiants doivent entrer leurs configurations et les tester sur les routeurs.

Phase 4 : Listes de contrôle d'accès

Cette Phase doit être effectuée après le Module 11.

C'est la partie la plus critique de l'étude de cas. Les étudiants doivent développer une liste de contrôle d'accès d'abord sur le papier, puis entrer la liste de contrôle d'accès dans une application de traitement de texte. Le professeur doit guider les étudiants tout au long du processus de copie et de collage des listes de contrôle d'accès dans la configuration de routeur.

Phase 5 : Documentation du réseau

Si les exigences en matière de documentation sont clairement énoncées dès le début, la Phase finale aura été exécutée tout au long de l'étude de cas. Cette phase permettra d'insister sur l'objectif de la documentation, qui doit être réalisée continuellement et révisée systématiquement.

Au cours de la dernière phase, la liste des travaux livrables doit être à nouveau abordée pour vérifier que l'étudiant a compris les exigences.

Facultatif

Il est possible, en supplément, d'ajouter une phase de réflexion pour que les étudiants puissent avoir un regard objectif sur cette étude de cas. Les questions

suivantes pourraient être posées : « Pourquoi deux types de documentation ? »,
« Que se passe-t-il si un équipement tombe en panne ? », etc.

Introduction

- En continuité des notions de base sur le réseau (CCNA 1), le CCNA 2 expose les notions de base sur les routeurs et le routage.
- L'Objectif du cours CCNA 2 est de fournir les compétences nécessaires à la compréhension des mécanismes de réseau avancés.
- A l'issue du cours CCNA2 l'étudiant est capable de :
 - Identifier les principales caractéristiques des technologies et des configurations
 - WAN courantes, ainsi que les différences avec les technologies LAN les plus répandues.
 - Décrire le rôle d'un routeur au sein d'un réseau WAN.
 - Décrire le rôle et le fonctionnement de la plate-forme logicielle Internet Operating System (IOS).
 - Établir la communication entre un équipement terminal et l'IOS du routeur, ainsi qu'utiliser l'IOS pour l'analyse système, la configuration et la réparation.
 - Identifier les principaux composants internes et externes d'un routeur, ainsi que décrire les fonctionnalités associées.
 - Connecter les ports console, WAN série et Fast Ethernet du routeur.
 - Définir, enregistrer et tester la configuration initiale d'un routeur.
 - Configurer des fonctions d'administration supplémentaires sur un routeur.
 - Découvrir et analyser le voisinage réseau depuis le routeur via la fonctionnalité de couche liaison de données intégrée depuis la console de routeur.
 - Utiliser les protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur.
 - Identifier les étapes de la séquence d'amorçage d'un routeur, ainsi que décrire l'impact des commandes "config-register" et "boot system" sur cette séquence.
 - Gérer les fichiers de configuration des équipements et de l'image système.
 - Décrire le fonctionnement du protocole ICMP (Internet Control Message Protocol), ainsi qu'identifier les raisons, les types et le format des messages de contrôle et d'erreur associés.

PHASE 1 : Description du projet :

Dans les vidéos, j'ai malheureusement fait des erreurs. Pour cette raison, il vaut mieux se fier à ce rapport.

La vidéo :

Le routage - phase 1 - 01 - description du projet.avi

Notre objectif de cette première phase est de mettre en place la configuration physique du réseau. Nous devons donc déterminer le type d'adresses réseau, le nombre de sous-réseaux nécessaires et le protocole de routage.

Afin de bien configurer les différents éléments, déterminons dans un premier temps le type d'adresses réseaux ou plutôt quelle classe d'adresse nous allons utiliser.

Nous avons un réseau privé d'entreprise donc nous aurons un adressage privé.

Plusieurs possibilités :

- classe A, avec la plage de 10.0.0.0 à 10.255.255.255

- ou classe B, avec la plage de 172.16.0.0 à 172.31.255.255

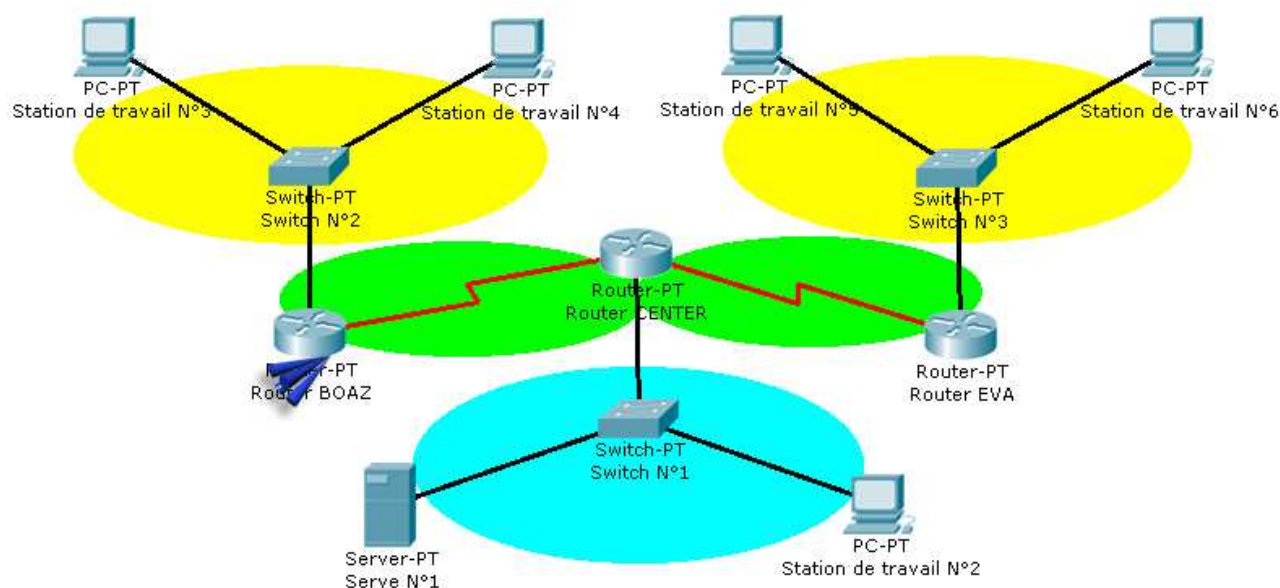
- ou classe C, avec la plage de 192.168.0.0 à 192.168.255.255

Une adresse IP de classe C dispose de trois octets pour identifier le réseau et d'un seul octet pour identifier les machines sur ce réseau. Ainsi, un réseau de classe C peut comporter jusqu'à (2^8-2) postes, soit 254 terminaux. Ce qui suffit dans cette configuration.

Dans un deuxième temps, déterminons le nombre de sous-réseaux :

Au regard du schéma, nous avons besoin de 5 sous-réseaux. (Cf. ellipses colorées)

(1 sous-réseau en bleu, 2 sous-réseaux distincts en vert et 2 sous-réseaux distincts en jaune)



Toute la simulation du réseau s'est effectuée sur le logiciel Packet Tracer 5.0.

Déterminons maintenant le protocole de routage.

Il existe des protocoles de routage interne et externe. Ici, seul le protocole interne est nécessaire.

Les IGP sont des protocoles fonctionnant à l'intérieur d'un système autonome.

Ces protocoles de routage interne fonctionnent de différentes façons :

- * Protocoles de routage à états de lien :
 - OSPF = Open Shortest Path First
 - IS-IS = Integrated Intermediate System to Intermediate System
- * Protocoles de routage à vecteurs de distance :
 - RIP = Routing Information Protocol
 - IGRP = Interior Gateway Routing Protocol
- * Protocoles hybride des deux premiers :
 - EIGRP = Enhanced Interior Gateway Routing Protocol

A première vue, chacun des cinq protocoles pourraient convenir. Etudions les avantages et inconvénients de chacun. Comparons les avantages et inconvénients des protocoles internes.

Procédons par élimination :

- déterminons quel protocole à états de liens nous retiendrions.
- déterminons quel protocole à vecteurs de distance nous retiendrions. (y compris le protocole Hybride EIGRP)

Pour cela, je m'aide des données que j'ai rassemblées sur Internet et de la documentation de la formation CISCO.

(Sources Internet : d'une présentation powerpoint de chez JUNIPER (un fabricant de routeur) et de diverses sources (laboratoire-microsoft.org, supinfo.com, Wikipedia.com, données universitaires françaises, ...) et Un article comparant les différents protocoles, d'après Brandon Teoh).

Après lecture approfondis des documents créons des tableaux afin de résumer les données de comparaisons. (Cf. Annexes : Comparaisons des protocoles de routage)

Nous retenons ainsi le protocole de routage OSPF.

(EIGRP serait aussi un bon choix. Nous l'utiliserons d'ailleurs si Packet tracer 5.0 ne gère pas l'OSPF et si ce dernier est trop complexe à mettre en œuvre)

Outre les avantages du Protocol OSPF, j'ai voulu le tester car son format non propriétaire et son paramétrage vaste, font de celui-ci un des protocoles qui commence à être de plus en plus utilisé, même sur des routeurs très pointus et marque reconnues.

En résumé, nous avons :

Une adresse privée de réseau de classe C de la plage de 192.168.0.0 à 192.168.255.255

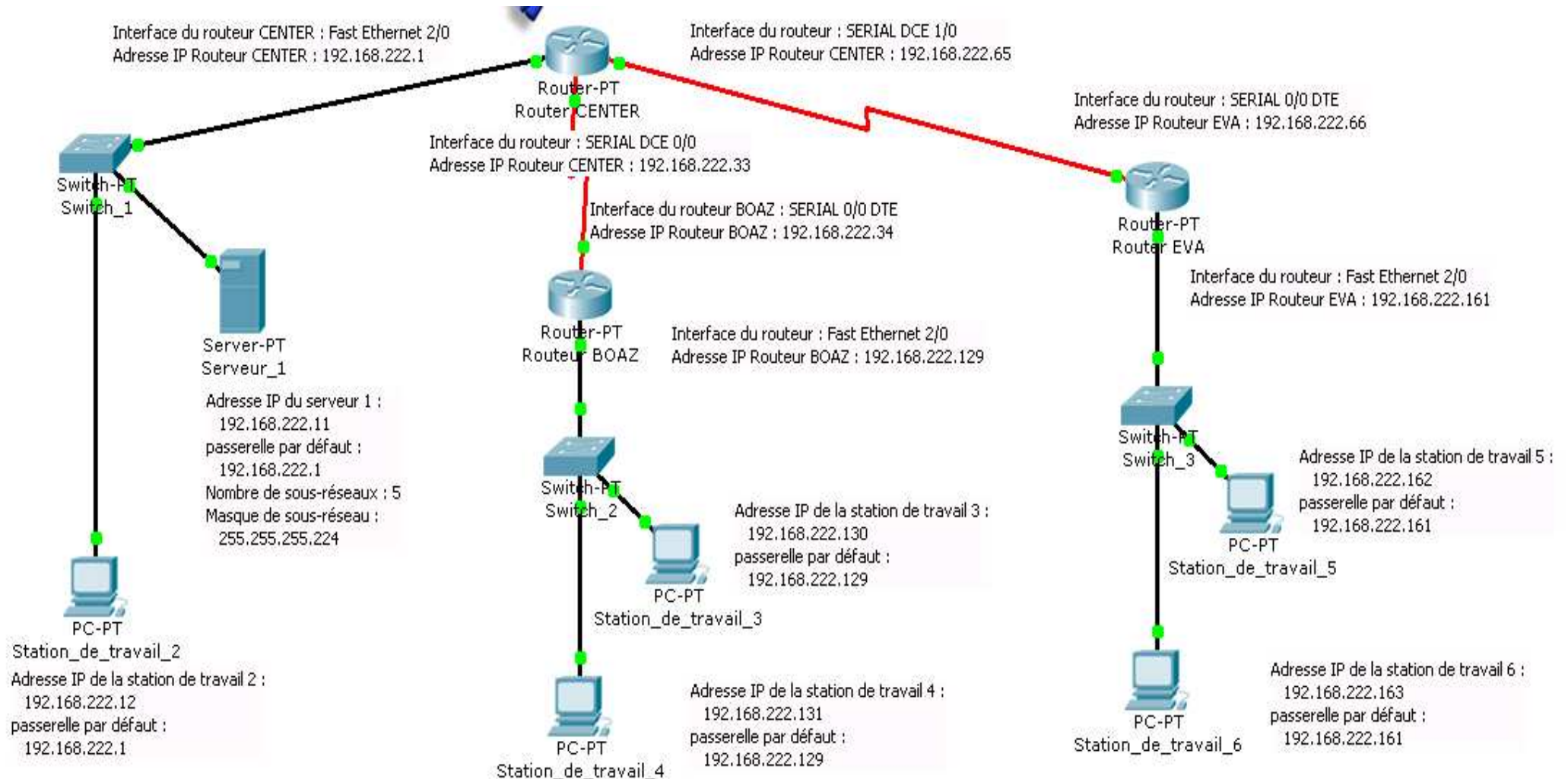
Le nombre de sous-réseaux nécessaires au nombre de : 5

Le protocole de routage : O.S.F.P. (Open Shortest Path First)

Nous pouvons dès à présent établir le plan partiel d'adressage IP du réseau.

(Attention, ce n'est que dans la phase 2 que nous pouvons réellement comme ci-dessous déterminer totalement les adresses IP de chaque interface appropriée).

Plan final d'adressage IP



PHASE 2: Adressage IP :

Les vidéos:

- Le routage - phase 2 - 01 - insertion de notes dans Packet tracer 5.0.avi*
- Le routage - phase 2 - 02 - choix réseau + masque.avi*
- Le routage - phase 2 - 03 - configuration éléments (stations de travail + serveur).avi*
- Le routage - phase 2 - 04 - répartition adresses IP.avi*
- Le routage - phase 2 - 05 - test éléments (sans routeur).avi*
- Le routage - phase 2 - 06 - suppression câblages routeurs par défaut.avi*
- Le routage - phase 2 - 07 - connexions routeur et cablage.avi*
- Le routage - phase 2 - 08 - ajustement connexions routeur et cablage.avi*
- Le routage - phase 2 - 09 - correction du nom des éléments.avi*

Il s'agit ici d'établir le sous-réseau. C'est-à-dire d'attribuer les adresses IP aux interfaces appropriées sur tous les routeurs et ordinateurs de l'inter-réseau.

1.1. Création du sous-réseau :

Au niveau de cette phase 2, nous avons :

- 5 sous-réseaux avec au maximum de 2 stations de travail par routeur.
- Un adressage privé de classe C, avec une plage d'adresse de sous-réseau offrant 254 postes de travail est largement suffisant.

Par exemple, une plage d'adressage privé de classe C de 192.168.222.1 à 192.168.222.254 conviendrait.

Explications :

La classe C correspond aux adresses du réseau 192.168.0.0, c'est-à-dire les adresses (la plage d'adresses utilisable) de réseau 192.168.0.1 à 223.255.255.254

(La première adresse d'un réseau spécifie le réseau lui-même, la dernière est une adresse de diffusion (ou adresse de broadcast)).

(Exemple ici : adresse du réseau correspond à 192.168.0.0 et l'adresse de diffusion est 223.255.255.255)

(Attention : ne pas confondre : "adresses du réseau ..." et "adresses de réseau ... à ...")

Cependant, ici, nous avons besoin d'un adressage privé.

La classe C correspondant aux adresses privées de 192.168.0.1 à 192.168.255.254

Ce qui laisse $2^8 - 2 = 255$ réseaux avec 254 stations de travail disponibles par réseau.

Dans notre cas, il n'y a besoin que d'une plage d'adresse C de réseau dans l'entreprise donc nous choisissons UNE plage parmi les 255 disponible. Par exemple : 192.168.222.1 à 192.168.222.254

1.2. Création du masque de sous-réseau :

Notre plage d'adressage privée de classe C, 192.168.222.1 à 192.168.222.254 a besoin d'un masque pour le filtrage des adresses.

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. le quatrième octet étant pour les hôtes.

(exemple : 192.168.255.255 s'écrit aussi 11000000.10101000.11111111.11111111)

Le nombre de sous-réseaux dépend du nombre de bits attribués en plus au réseau. C'est-à-dire, qu'une partie des bits de l'octet réservé aux hôtes est utilisé pour définir le nombre de sous-réseau.

Nombre de bits	1	2	3	4	5	6
Nombre de sous-réseaux	2	4	8	16	32	64

Dans notre cas, nous avons besoin de 5 sous-réseaux, donc nous devons réserver une adresse de classe C avec un minimum de 3 bits sur le 4ème octet.

Prenons donc 192. 168. 222. 1 (notation décimale)
11000000. 10101000. 11011110. 00000001 (notation binaire)

Le masque à appliquer sera alors : 255 .255 .255 .224 (n. décimale)
11111111.11111111.11111111.11100000 (n. binaire)

d'où :

ET LOGIQUE 11000000.10101000.11011110.00000001
= 11111111.11111111.11111111.11100000
= 11000000.10101000.11011110.00000001 (soit 192.168.222.0)

(11000000.10101000.11011110.00000001 est aussi noté aussi /27 car il y a 27 bits pour le découpage du réseau en sous-réseaux)

En réalité, il y a donc 8 plages possibles pour le résultat du masquage de cette adresse IP :

- * Soit les 3 premiers bits du 4ème octet sont 000, auquel cas le résultat du masquage est 192.168.222.0
- * Soit les 3 premiers bits du 4ème octet sont 001, auquel cas le résultat du masquage est 192.168.222.32
- * Soit les 3 premiers bits du 4ème octet sont 010, auquel cas le résultat du masquage est 192.168.222.64
- * Soit les 3 premiers bits du 4ème octet sont 011, auquel cas le résultat du masquage est 192.168.222.96
- * Soit les 3 premiers bits du 4ème octet sont 100, auquel cas le résultat du masquage est 192.168.222.128
- * Soit les 3 premiers bits du 4ème octet sont 101, auquel cas le résultat du masquage est 192.168.222.160
- * Soit les 3 premiers bits du 4ème octet sont 110, auquel cas le résultat du masquage est 192.168.222.192
- * Soit les 3 premiers bits du 4ème octet sont 111, auquel cas le résultat du masquage est 192.168.222.224
- * Soit les 3 premiers bits du 4ème octet sont 111, auquel cas le résultat du masquage est 192.168.222.255

En conclusion :

Nous avons donc un réseau d'adresse IP de 192.168.222.0/27. Nous avons le choix entre 8 plages d'adresses de sous-réseau pour les 5 sous-réseaux nécessaires.

PHASE 1 : DESCRIPTION DU PROJET

PHASE 2 : ADRESSAGE IP

		Commentaires
Adresse du réseau :	Classe C	192.168.0.0
Adresses de réseau :	Classe C	192.168.0.1 à 223.255.255.254
Adresse retenue du réseau :	Classe C (privée)	192.168.222.0
Adresses retenue de réseau :	Classe C (privée)	192.168.222.0 à 192.168.222.254
Masque de sous-réseau :	255.255.255.224	3 bits sur le 4ème octet donc masque en /27
		adresse du réseau : 192.168.222.0 /27
Nombre de sous-réseaux nécessaire :	5	nombre de sous-réseaux disponibles = 8
Nombre de bits réseau :	27	11111111.11111111.11111111.11100000
Nombre de bits hôtes :	5	00000000.00000000.00000000.00011111
Nombre d'hôtes par sous-réseau	30	
Protocole de routage :	OSPF	autres possibilités : RIP, IGP, EIGRP

Plages d'adresses de réseau / adresse du sous-réseau / adresse de diffusion				
Plage d'adresse de réseau		Adresse du sous-réseau	Adresse de diffusion	Plage retenue
début	fin	début	fin	
192.168.222.1/27	192.168.222.30/27	192.168.222.0	192.168.222.31	oui
192.168.222.33/27	192.168.222.62/27	192.168.222.32	192.168.222.63	oui
192.168.222.65/27	192.168.222.94/27	192.168.222.64	192.168.222.95	oui
192.168.222.97/27	192.168.222.126/27	192.168.222.96	192.168.222.127	non
192.168.222.129/27	192.168.222.158/27	192.168.222.128	192.168.222.159	oui
192.168.222.161/27	192.168.222.190/27	192.168.222.160	192.168.222.191	oui
192.168.222.193/27	192.168.222.222/27	192.168.222.192	192.168.222.223	non
192.168.222.225/27	192.168.222.254/27	192.168.222.224	192.168.222.255	non

Par rapport au choix des adresses IP pour le sous-réseau Fast Ethernet du routeur CENTER, j'ai volontairement choisis de ne pas attribuer les IP de 192.168.222.1 à 192.168.222.3. Mais plutôt 192.168.222.1 au routeur, 192.168.222.11 pour le serveur 1 de fichier et 192.168.222.12 à la station de travail 2.

Pour les sous-réseaux entre les routeurs, les plages d'adresses du sous-réseau suivant ont été attribuées : 192.168.222.64 /27 et 192.168.222.128 /27

Pour les sous-réseaux Fast Ethernet des routeurs les plages d'adresses du sous-réseau suivantes : 192.168.222.128 /27 et 192.168.222.160 /27

J'ai ignoré la plage d'adresses du sous-réseau suivant : 192.168.222.96 /27

Avec le recul, je pense qu'il aurait été plus judicieux de garder une continuité de numérotation de l'adressage IP.

PHASE 3 : Configuration de base des routeurs et des stations de travail :

Les videos :

Le routage - phase 3 - 01 - configuration générale des routeurs.avi

Le routage - phase 3 - 02 - configuration des interfaces.avi

Le routage - phase 3 - 03 - configuration des réseaux.avi

Le routage - phase 3 - 04 - configuration des hotes.avi

Le routage - phase 3 - 05 - insertion d'une bannière.avi

Le routage - phase 3 - 06 - phase de test.avi

Les tableaux des pages suivantes exposent le choix de la configuration des routeurs et des stations de travail.

A retenir :

- Lorsque deux routeurs adjacents sont connectés sur le port série, l'un est en DCE, et l'autre est en DTE
- Pour relier deux routeurs directement, il faut utiliser le port série (ex : SERIAL 0/0)
- Pour relier un routeur directement au switch, il faut utiliser le port Fast Ethernet (ex : Fast Ethernet 0/0)
- Par simplicité, la numérotation du dernier octet est croissante de plus « 1 » d'une station de travail à l'autre. Il est préférable en général d'avoir un adressage continu.
- Nous avons besoin sur les routeurs de 2 ports Série et de 2 ports Fast Ethernet (même si tous ne sont pas utilisés). Le branchement ne peut se faire que si le routeur est éteint.
- Lors de la configuration des adresses IP des hôtes ou des interfaces sur les routeurs (nous verrons cela bien après), il ne faut pas que les noms des éléments comportent des espaces :
ex : "Station de travail N°2" est renommée en "station_de_travail_2"

PHASE 3 : CONFIGURATION DE BASE DES ROUTEURS ET DES STATIONS DE TRAVAIL

	Routeur BOAZ	Routeur CENTER	Routeur EVA
Nom d'hôte	BOAZ	CENTER	EVA
Mot de passe de console	cons_boaz	cons_center	cons_eva
Mot de passe "enable secret"	sec_boaz	sec_center	sec_eva
Mot de passe VTY	vty_boaz	vty_center	vty_eva
Adresse IP Serial 0/0	192.168.222.34	192.168.222.33	192.168.222.66
Adresse IP Serial 1/0	non connecté !	192.168.222.65	non connecté !
Fréquence d'horloge Serial 0/0	aucune	CLOCKRATE 56000	aucune
Fréquence d'horloge Serial 1/0	aucune	CLOCKRATE 56000	aucune
Adresse IP Fa 2/0	192.168.222.129	192.168.222.1	192.168.222.161
Adresse IP Fa 3/0	non connecté !	non connecté !	non connecté !
Activer les interfaces	NO SHUTDOWN	NO SHUTDOWN	NO SHUTDOWN
Ajouter un protocole de routage	OSPF	OSPF	OSPF
Ajouter des instructions réseau (adresse réseau suivi de son masque générique)	network 192.168.222.32 0.0.0.255 area 222 network 192.168.222.128 0.0.0.255 area 222	network 192.168.222.0 0.0.0.255 area 222 network 192.168.222.32 0.0.0.255 area 222 network 192.168.222.64 0.0.0.255 area 222	network 192.168.222.160 0.0.0.255 area 222 network 192.168.222.64 0.0.0.255 area 222

Table d'interfaces (Normalement, il suffit de donner les interfaces directes)	ip address 192.168.222.34 255.255.255.224	ip address 192.168.222.33 255.255.255.224	ip address 192.168.222.66 255.255.255.224
		ip address 192.168.222.65 255.255.255.224	
	ip address 192.168.222.129 255.255.255.224	ip address 192.168.222.1 255.255.255.224	ip address 192.168.222.161 255.255.255.224
Table d'hôtes (pour des raisons de facilité, il est intéressant que tous les routeurs dans un petit réseau est la même table de routage)	Ip host CENTER 192.168.222.1	Ip host CENTER 192.168.222.1	Ip host CENTER 192.168.222.1
	Ip host CENTER 192.168.222.33	Ip host CENTER 192.168.222.33	Ip host CENTER 192.168.222.33
	Ip host CENTER 192.168.222.65	Ip host CENTER 192.168.222.65	Ip host CENTER 192.168.222.65
	Ip host BOAZ 192.168.222.34	Ip host BOAZ 192.168.222.34	Ip host BOAZ 192.168.222.34
	Ip host EVA 192.168.222.66	Ip host EVA 192.168.222.66	Ip host EVA 192.168.222.66

Message du jour	AUTHORIZED ACCESS ONLY	AUTHORIZED ACCESS ONLY	AUTHORIZED ACCESS ONLY
Description Serial 0/0	Interface série n°0, DTE, d'adresse IP 192.168.222.34, connecté à l'interface série n°0, DCE, du routeur CENTER, d'adresse IP 192.168.222.33)	Interface série n°0, DCE, d'adresse IP 192.168.222.33, connecté à l'interface série n°0, DTE, du routeur CENTER, d'adresse IP 192.168.222.34)	Interface série n°0, DTE, d'adresse IP 192.168.222.66, connecté à l'interface série n°1, DCE, du routeur CENTER, d'adresse IP 192.168.222.65)
Description Serial 1/0		Interface série n°1, DCE, d'adresse IP 192.168.222.65, connecté à l'interface série n°0, DTE, du routeur EVA, d'adresse IP 192.168.222.66)	
Description Fa 2/0	Interface Fast Ethernet, d'adresse IP 192.168.222.129, connecté à l'interface Fast Ethernet n°0/1, du Switch n°2	Interface Fast Ethernet, d'adresse IP 192.168.222.1, connecté à l'interface Fast Ethernet n°2/1, du Switch n°1	Interface Fast Ethernet, d'adresse IP 192.168.222.161, connecté à l'interface Fast Ethernet n°0/1, du Switch n°3
Description Fa 3/0	non connecté !	non connecté !	non connecté !

PHASE 4 : Listes de contrôle d'accès :

Les videos :

Le routage - phase 4 - 01 - démarche générale de l'ACL.avi

Le routage - phase 4 - 02 - ACL du routeur CENTER.avi

Le routage - phase 4 - 03 - ACL du routeur BOAZ.avi

Le routage - phase 4 - 04 - ACL du routeur EVA.avi

Le routage - phase 4 - 05 - ACL - test et corrections.avi

Après lecture de la documentation, nous pouvons établir la démarche de création des Listes de contrôle d'accès.

Nous prendrons de préférence des ACL nommées. La gestion se fera au plus proche de la source (souvent sur les interfaces d'entrées des équipements hôtes vers le routeur). Les ACL nommées permettent une plus grande souplesse lors de modifications du réseau.

(Cependant, cette version de packet tracer 5.0 ne permet pas d'utiliser correctement les noms. Nous utiliserons donc simplement des ACL étendues (avec des numéros seulement))

Méthode :

- 1.) A la source du routeur, noter en face de chaque interface ce qui doit être bloqué avec les autorisations spécifiques.
- 2.) De même, noter ce qui est autorisé avec les autorisations spécifiques.

En bilan après lecture :

- tous les routeurs ont permission d'accès sur tout équipement.
- "serveur 1" et "station de travail 2" ont permission d'accès sur tout équipement.
- le "sous-réseau Boaz" et le "sous-réseau Eva" ont permission d'accès seulement sur leur sous-réseau respectif
- cependant:
 - "station de travail 3" peut accéder (requête de ping uniquement) à "station de travail 6"
 - "station de travail 4" ne peut pas accéder à "routeur EVA" en connexion Telnet

A savoir :

- Une requête de ping est différente d'une connexion. La requête de ping à un caractère "unidirectionnel", dans le sens où il n'y a pas connexion "bidirectionnelle".
- Il est important de savoir que, implicitement, à la fin d'une liste de contrôle d'accès, l'instruction "deny ip any any" existe. Ce qui a pour effet de refuser toute connexion ne répondant pas aux exigences des lignes d'instructions précédentes. il est intéressant de donner un caractère explicite en écrivant cette instruction en fin de liste.

	ACCESS LISTS	INTERFACES																														
ROUTEUR CENTER	« Il n'est pas nécessaire d'en mettre ! mais nous pouvons (certes inutilement préciser) : » Extended IP access list 111 permit ip any any	<table><tr><th>Interface</th><th>IP-Address</th><th>OK?</th><th>Method</th><th>Status</th><th>Protocol</th></tr><tr><td>Serial0/0</td><td>192.168.222.34</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>Serial1/0</td><td>unassigned</td><td>YES</td><td>manual</td><td>administratively down</td><td>down</td></tr><tr><td>FastEthernet2/0</td><td>192.168.222.129</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>FastEthernet3/0</td><td>unassigned</td><td>YES</td><td>manual</td><td>administratively down</td><td>down</td></tr></table>	Interface	IP-Address	OK?	Method	Status	Protocol	Serial0/0	192.168.222.34	YES	manual	up	up	Serial1/0	unassigned	YES	manual	administratively down	down	FastEthernet2/0	192.168.222.129	YES	manual	up	up	FastEthernet3/0	unassigned	YES	manual	administratively down	down
Interface	IP-Address	OK?	Method	Status	Protocol																											
Serial0/0	192.168.222.34	YES	manual	up	up																											
Serial1/0	unassigned	YES	manual	administratively down	down																											
FastEthernet2/0	192.168.222.129	YES	manual	up	up																											
FastEthernet3/0	unassigned	YES	manual	administratively down	down																											
ROUTEUR EVA	Extended IP access list 160 permit icmp 192.168.222.160 0.0.0.31 192.168.222.64 0.0.0.31 echo-reply permit icmp 192.168.222.160 0.0.0.31 192.168.222.32 0.0.0.31 echo-reply permit icmp 192.168.222.160 0.0.0.31 host 192.168.222.11 permit icmp 192.168.222.160 0.0.0.31 host 192.168.222.12 echo-reply permit icmp 192.168.222.160 0.0.0.31 host 192.168.222.161 echo-reply permit icmp host 192.168.222.163 host 192.168.222.130 echo-reply deny ip any any	<table><tr><th>Interface</th><th>IP-Address</th><th>OK?</th><th>Method</th><th>Status</th><th>Protocol</th></tr><tr><td>Serial0/0</td><td>192.168.222.33</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>Serial1/0</td><td>192.168.222.65</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>FastEthernet2/0</td><td>192.168.222.1</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>FastEthernet3/0</td><td>unassigned</td><td>YES</td><td>manual</td><td>administratively down</td><td>down</td></tr></table>	Interface	IP-Address	OK?	Method	Status	Protocol	Serial0/0	192.168.222.33	YES	manual	up	up	Serial1/0	192.168.222.65	YES	manual	up	up	FastEthernet2/0	192.168.222.1	YES	manual	up	up	FastEthernet3/0	unassigned	YES	manual	administratively down	down
Interface	IP-Address	OK?	Method	Status	Protocol																											
Serial0/0	192.168.222.33	YES	manual	up	up																											
Serial1/0	192.168.222.65	YES	manual	up	up																											
FastEthernet2/0	192.168.222.1	YES	manual	up	up																											
FastEthernet3/0	unassigned	YES	manual	administratively down	down																											
ROUTEUR BOAZ	Extended IP access list 128 permit icmp 192.168.222.128 0.0.0.31 host 192.168.222.129 echo-reply permit icmp 192.168.222.128 0.0.0.31 192.168.222.32 0.0.0.31 echo-reply permit icmp 192.168.222.128 0.0.0.31 192.168.222.64 0.0.0.31 echo-reply permit ip 192.168.222.128 0.0.0.31 host 192.168.222.11 permit icmp 192.168.222.128 0.0.0.31 host 192.168.222.12 echo-reply permit ip host 192.168.222.130 host 192.168.222.163 deny ip any any	<table><tr><th>Interface</th><th>IP-Address</th><th>OK?</th><th>Method</th><th>Status</th><th>Protocol</th></tr><tr><td>Serial0/0</td><td>192.168.222.66</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>Serial1/0</td><td>unassigned</td><td>YES</td><td>manual</td><td>administratively down</td><td>down</td></tr><tr><td>FastEthernet2/0</td><td>192.168.222.161</td><td>YES</td><td>manual</td><td>up</td><td>up</td></tr><tr><td>FastEthernet3/0</td><td>unassigned</td><td>YES</td><td>manual</td><td>administratively down</td><td>down</td></tr></table>	Interface	IP-Address	OK?	Method	Status	Protocol	Serial0/0	192.168.222.66	YES	manual	up	up	Serial1/0	unassigned	YES	manual	administratively down	down	FastEthernet2/0	192.168.222.161	YES	manual	up	up	FastEthernet3/0	unassigned	YES	manual	administratively down	down
Interface	IP-Address	OK?	Method	Status	Protocol																											
Serial0/0	192.168.222.66	YES	manual	up	up																											
Serial1/0	unassigned	YES	manual	administratively down	down																											
FastEthernet2/0	192.168.222.161	YES	manual	up	up																											
FastEthernet3/0	unassigned	YES	manual	administratively down	down																											

PHASE 5 : Documentation du réseau :

Pour des soucis de compréhension des informations des routeurs, j'ai préféré réduire volontairement la taille des caractères.
Une version informatique plus nette sur tableur (*.xls / non imprimé) est également disponible.

	Routeur BOAZ	Routeur CENTER	Routeur EVA
show cdp neighbors	Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Device ID Local Intrfce Holdtme Capability Platform Port ID CENTER Ser 0/0 174 R PT1000 Ser 0/0 Switch Fas 2/0 174 S PT3000 Fas 0/1	Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Device ID Local Intrfce Holdtme Capability Platform Port ID Switch Fas 2/0 172 S PT3000 Fas 2/1 BOAZ Ser 0/0 172 R PT1000 Ser 0/0 EVA Ser 1/0 172 R PT1000 Ser 0/0	Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Device ID Local Intrfce Holdtme Capability Platform Port ID Switch Fas 2/0 140 S PT3000 Fas 0/1 CENTER Ser 0/0 140 R PT1000 Ser 1/0
show ip route	Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is not set 192.168.222.0/27 is subnetted, 5 subnets O 192.168.222.0 [110/782] via 192.168.222.33, 00:22:49, Serial0/0 C 192.168.222.32 is directly connected, Serial0/0 O 192.168.222.64 [110/1562] via 192.168.222.33, 00:22:49, Serial0/0 C 192.168.222.128 is directly connected, FastEthernet2/0 O 192.168.222.160 [110/1563] via 192.168.222.33, 00:22:39, Serial0/0	Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is not set 192.168.222.0/27 is subnetted, 5 subnets C 192.168.222.0 is directly connected, FastEthernet2/0 C 192.168.222.32 is directly connected, Serial0/0 C 192.168.222.64 is directly connected, Serial1/0 O 192.168.222.128 [110/782] via 192.168.222.34, 00:09:17, Serial0/0 O 192.168.222.160 [110/782] via 192.168.222.66, 00:09:17, Serial1/0	Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is not set 192.168.222.0/27 is subnetted, 5 subnets O 192.168.222.0 [110/782] via 192.168.222.65, 00:33:54, Serial0/0 O 192.168.222.32 [110/1562] via 192.168.222.65, 00:33:54, Serial0/0 C 192.168.222.64 is directly connected, Serial0/0 O 192.168.222.128 [110/1563] via 192.168.222.65, 00:33:54, Serial0/0 C 192.168.222.160 is directly connected, FastEthernet2/0

show ip protocols	Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 192.168.222.129 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 192.168.222.0 0.0.0.255 area 222 Routing Information Sources: Gateway Distance Last Update 192.168.222.33 110 00:24:00 Distance: (default is 110)	Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 192.168.222.65 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 192.168.222.0 0.0.0.255 area 222 Routing Information Sources: Gateway Distance Last Update 192.168.222.34 110 00:11:21 192.168.222.66 110 00:11:21 Distance: (default is 110)	Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 192.168.222.161 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 192.168.222.0 0.0.0.255 area 222 Routing Information Sources: Gateway Distance Last Update 192.168.222.65 110 00:04:20 Distance: (default is 110)
show ip interface brief	Interface IP-Address OK? Method Status Protocol Serial0/0 192.168.222.34 YES manual up up Serial1/0 unassigned YES manual administratively down down FastEthernet2/0 192.168.222.129 YES manual up up FastEthernet3/0 unassigned YES manual administratively down down	Interface IP-Address OK? Method Status Protocol Serial0/0 192.168.222.33 YES manual up up Serial1/0 192.168.222.65 YES manual up up FastEthernet2/0 192.168.222.1 YES manual up up FastEthernet3/0 unassigned YES manual administratively down down	Interface IP-Address OK? Method Status Protocol Serial0/0 192.168.222.66 YES manual up up Serial1/0 unassigned YES manual administratively down down FastEthernet2/0 192.168.222.161 YES manual up up FastEthernet3/0 unassigned YES manual administratively down down

show version	Cisco Internetwork Operating System Software IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Wed 27-Apr-04 19:01 by miwang Image text-base: 0x8000808C, data-base: 0x80A1FECC ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1) Copyright (c) 2000 by cisco Systems, Inc. ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) System returned to ROM by reload System image file is "flash:pt1000-i-mz.122-28.bin" PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory . Processor board ID PT0123 (0123) PT2005 processor: part number 0, mask 01 Bridging software. X.25 software, Version 3.0.0. 2 FastEthernet/IEEE 802.3 interface(s) 2 Low-speed serial(sync/async) network interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write) Configuration register is 0x2102	Cisco Internetwork Operating System Software IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Wed 27-Apr-04 19:01 by miwang Image text-base: 0x8000808C, data-base: 0x80A1FECC ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1) Copyright (c) 2000 by cisco Systems, Inc. ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) System returned to ROM by reload System image file is "flash:pt1000-i-mz.122-28.bin" PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory . Processor board ID PT0123 (0123) PT2005 processor: part number 0, mask 01 Bridging software. X.25 software, Version 3.0.0. 2 FastEthernet/IEEE 802.3 interface(s) 2 Low-speed serial(sync/async) network interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write) Configuration register is 0x2102	Cisco Internetwork Operating System Software IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Wed 27-Apr-04 19:01 by miwang Image text-base: 0x8000808C, data-base: 0x80A1FECC ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1) Copyright (c) 2000 by cisco Systems, Inc. ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) System returned to ROM by reload System image file is "flash:pt1000-i-mz.122-28.bin" PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory . Processor board ID PT0123 (0123) PT2005 processor: part number 0, mask 01 Bridging software. X.25 software, Version 3.0.0. 2 FastEthernet/IEEE 802.3 interface(s) 2 Low-speed serial(sync/async) network interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write) Configuration register is 0x2102
-------------------------	---	---	---

show hosts	Default Domain is not set Name/address lookup uses domain service Name servers are 255.255.255.255 Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate temp - temporary, perm - permanent NA - Not Applicable None - Not defined Host Port Flags Age Type Address(es) boaz None (perm, OK) 0 IP 192.168.222.34 center None (perm, OK) 0 IP 192.168.222.65 eva None (perm, OK) 0 IP 192.168.222.66	CENTER#show hosts Default Domain is not set Name/address lookup uses domain service Name servers are 255.255.255.255 Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate temp - temporary, perm - permanent NA - Not Applicable None - Not defined Host Port Flags Age Type Address(es) boaz None (perm, OK) 0 IP 192.168.222.34 center None (perm, OK) 0 IP 192.168.222.65 eva None (perm, OK) 0 IP 192.168.222.66	Default Domain is not set Name/address lookup uses domain service Name servers are 255.255.255.255 Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate temp - temporary, perm - permanent NA - Not Applicable None - Not defined Host Port Flags Age Type Address(es) boaz None (perm, OK) 0 IP 192.168.222.34 center None (perm, OK) 0 IP 192.168.222.65 eva None (perm, OK) 0 IP 192.168.222.66
	BOAZ#show startup-config Using 1284 bytes ! version 12.2 no service password-encryption ! hostname BOAZ ! ! enable secret 5 \$1\$mERr\$vDYdgoVXI064kePUMy9V40 ! ! ! ! ! ip ssh version 1 ip host boaz 192.168.222.34 ip host center 192.168.222.65 ip host eva 192.168.222.66 ! ! interface Serial0/0 ip address 192.168.222.34 255.255.255.224 ! interface Serial1/0 no ip address shutdown ! interface FastEthernet2/0 ip address 192.168.222.129 255.255.255.224	Using 815 bytes ! version 12.2 no service password-encryption ! hostname CENTER ! ! enable secret 5 \$1\$mERr\$LYZnexR9L8NAnqrWHR0bp1 ! ! ! ! ip ssh version 1 ip host boaz 192.168.222.34 ip host center 192.168.222.65 ip host eva 192.168.222.66 ! ! interface Serial0/0 ip address 192.168.222.33 255.255.255.224 clock rate 56000 ! interface Serial1/0 ip address 192.168.222.65 255.255.255.224 clock rate 56000 ! interface FastEthernet2/0 ip address 192.168.222.1 255.255.255.224	Using 1321 bytes ! version 12.2 no service password-encryption ! hostname EVA ! ! enable secret 5 \$1\$mERr\$K02HINf30gi9ar2Nz9oGM0 ! ! ! ! ip ssh version 1 ip host boaz 192.168.222.34 ip host center 192.168.222.65 ip host eva 192.168.222.66 ! ! interface Serial0/0 ip address 192.168.222.66 255.255.255.224 ! interface Serial1/0 no ip address shutdown ! interface FastEthernet2/0 ip address 192.168.222.161 255.255.255.224 ip access-group 160 in

<pre> ip access-group 128 in duplex auto speed auto ! interface FastEthernet3/0 no ip address duplex auto speed auto shutdown ! router ospf 1 log-adjacency-changes network 192.168.222.0 0.0.0.255 area 222 ! ip classless ! ! access-list 128 permit icmp 192.168.222.128 0.0.0.31 host 192.168.222.129 echo-reply access-list 128 permit icmp 192.168.222.128 0.0.0.31 192.168.222.32 0.0.0.31 echo-reply access-list 128 permit icmp 192.168.222.128 0.0.0.31 192.168.222.64 0.0.0.31 echo-reply access-list 128 permit ip 192.168.222.128 0.0.0.31 host 192.168.222.11 access-list 128 permit icmp 192.168.222.128 0.0.0.31 host 192.168.222.12 echo-reply access-list 128 permit ip host 192.168.222.130 host 192.168.222.163 access-list 128 deny ip any any ! ! ! banner motd ^AUTHORIZED ACCESS ONLY^C line con 0 password cons_boaz login line vty 0 4 password vty_boaz login ! ! end </pre>	<pre> duplex auto speed auto ! interface FastEthernet3/0 no ip address duplex auto speed auto shutdown ! router ospf 1 log-adjacency-changes network 192.168.222.0 0.0.0.255 area 222 ! router rip ! ip classless ! ! ! banner motd ^AUTHORIZED ACCESS ONLY^C line con 0 password cons_center login line vty 0 4 password vty_center login ! ! ! end </pre>	<pre> ip access-group EVA out duplex auto speed auto ! interface FastEthernet3/0 no ip address duplex auto speed auto shutdown ! router ospf 1 log-adjacency-changes network 192.168.222.0 0.0.0.255 area 222 ! ip classless ! ! access-list 160 permit icmp 192.168.222.160 0.0.0.31 192.168.222.64 0.0.0.31 echo-reply access-list 160 permit icmp 192.168.222.160 0.0.0.31 192.168.222.32 0.0.0.31 echo-reply access-list 160 permit icmp 192.168.222.160 0.0.0.31 host 192.168.222.11 access-list 160 permit icmp 192.168.222.160 0.0.0.31 host 192.168.222.12 echo-reply access-list 160 permit icmp 192.168.222.160 0.0.0.31 host 192.168.222.161 echo-reply access-list 160 permit icmp host 192.168.222.163 host 192.168.222.130 echo-reply access-list 160 deny ip any any ! ! ! banner motd ^AUTHORIZED ACCESS ONLY^C line con 0 password cons_eva login line vty 0 4 password vty_eva login ! ! ! end </pre>
---	---	---

Conclusion et réflexion :

Cette étude de cas est tout à fait intéressante car elle permet au travers d'une manipulation pratique de synthétiser les aspects de la configuration et du dépannage sur les routeurs.

De plus, les séquences détaillées en phases permettent de bien assimiler les étapes d'approches et de résolutions de la construction de l'infrastructure d'un exemple de réseau.

Au fur et à mesure de l'avancement dans cette étude de cas, de nombreuses phases de tests sur la construction du réseau ont permis de vérifier la concordance de l'ajout de notions, d'ordre topologique, matérielle, de gestion et de sécurité. Ces phases de test sont à mon avis très intéressantes pour développer un sens critique des erreurs à ne pas commettre ou des pannes qui pourraient survenir.

J'ai pris soin, tout au long de la configuration du réseau et particulièrement des routeurs, de créer des vidéos des différentes manipulations. Cela dans un but pédagogique et d'entraide. Ces vidéos comportent toutes une zone d'explication des manipulations au fur et à mesure de l'avancement de la réflexion et des tâches à accomplir. Ces vidéos montrent aussi les erreurs que l'on peut faire et comment les corriger. A défaut d'être spécifiquement professionnelle, je pense qu'elles peuvent constituer une approche intéressante sous forme d'un tutoriel.

Dans les vidéos, j'ai malheureusement fait des erreurs. Pour cette raison, il vaut mieux se fier à ce rapport.

Ainsi, beaucoup d'explications de la démarche et de justifications de certains choix sont plus sous forme vidéo que par écrit sur ce présent rapport. Néanmoins, toutes les notes des vidéos sont en Annexes.

Maintenant, si nous regardons d'un peu plus près la mise en œuvre de ce réseau dans un cas réel d'entreprise, nous pourrions développer les points suivant :

- Le nombre de stations de travail par rapport aux routeurs est vraiment faible. Je pense que l'intérêt est donc plus basé sur la compréhension des notions de routage. Il n'est pas simple non plus de réellement simuler une mise en œuvre dans une salle de travaux pratique. Un seul routeur et un seul switch suffiraient à réaliser correctement ce réseau si l'on se base sur le nombre de postes de travail. Mais l'objectif pédagogique ne serait pas le même.
- Aussi, il n'y pas de prise en compte d'une liaison vers l'extérieur de l'entreprise (par exemple Internet). Cela aurait pu ajouter des paramètres intéressants de configuration de routage.

- Dans ce schéma, nous voyons très bien que le routeur CENTER occupe une position centrale dans la répartition des données. Si ce dernier venait à avoir un problème technique, tout le réseau serait bloqué. Une configuration avec une approche plus en triangulation (avec des chemins parallèles) serait une piste intéressante.

Par exemple, nous pourrions ajouter une liaison série directe entre les routeurs EVA et BOAZ. Et à cela, ajouté une liaison respective Fast Ethernet entre le Switch 1 et chacun des routeurs EVA et BOAZ. Ceci sécuriserait plus le réseau en cas d'une éventuelle panne sur une connexion. Le degré de panne pourrait être de l'ordre de 3 liaisons sur le routeur CENTER, sans affecter l'échange de données. Je n'épilouerais pas ici sur les autres cas possibles.

- Toujours dans le domaine des pannes techniques, la création au préalable d'une documentation du réseau fonctionnant correctement est primordiale. En effet, plus celle-ci est complète, meilleure peut être une reprise après incident. Il faut une documentation sur la topologie du réseau, une sur la gestion de la configuration et une sur la gestion de la sécurité. Ces deux dernières doivent permettre de réactiver une configuration fonctionnelle dans les meilleurs délais. De plus, une documentation sur la gestion de la sécurité est obligatoire, afin de préserver confidentialité et risque minimum des problèmes divers de détraquement du réseau. De plus, une gestion de la sécurité ne va pas à l'encontre d'une exploitation optimum du réseau.

En conclusion, je tiens à souligner que je comprends mieux la notion développée par CISCO dans le titre de ce CCNA : « les notions de base sur les routeurs et le routage ». En effet, c'est un domaine avec encore plein d'inconnus pour moi. Domaine qui m'a plutôt effrayé au début, mais qui devient agréable et moins difficile d'approche avec l'expérience. J'espère pouvoir par la suite, dépasser les notions « de base » et donc approfondir des notions « avancées ».

ANNEXES

Compilation des vidéos

Comparaisons des protocoles de routage

Le protocole OSPF

Adressage IP et configuration des routeurs

Commentaires des vidéos

Compilation des vidéos

Temps total : 2 h 55 min 42 s

Taille totale : 317 MO

Le routage - phase 1 - 01 - description du projet.avi (03:41)

Le routage - phase 2 - 01 - insertion de notes dans Packet tracer 5.0.avi (00:29)

Le routage - phase 2 - 02 - choix réseau + masque.avi (04:52)

Le routage - phase 2 - 03 - configuration éléments (stations de travail + serveur).avi (04 :17)

Le routage - phase 2 - 04 - répartition adresses IP.avi (05:58)

Le routage - phase 2 - 05 - test éléments (sans routeur).avi (03:37)

Le routage - phase 2 - 06 - suppression câblages routeurs par défaut.avi (01:57)

Le routage - phase 2 - 07 - connexions routeur et cablage.avi (05:05)

Le routage - phase 2 - 08 - ajustement connexions routeur et cablage.avi (02:16)

Le routage - phase 2 - 09 - correction du nom des éléments.avi (02:33)

Le routage - phase 3 - 01 - configuration générale des routeurs.avi (43:41)

Le routage - phase 3 - 02 - configuration des interfaces.avi (17:00)

Le routage - phase 3 - 03 - configuration des réseaux.avi (04:00)

Le routage - phase 3 - 04 - configuration des hotes.avi (06:44)

Le routage - phase 3 - 05 - insertion d'une bannière.avi (05:50)

Le routage - phase 3 - 06 - phase de test.avi (08:42)

Le routage - phase 4 - 01 - démarche générale de l'ACL.avi (04:24)

Le routage - phase 4 - 02 - ACL du routeur CENTER.avi (00:30)

Le routage - phase 4 - 03 - ACL du routeur BOAZ.avi (1 :25)

Le routage - phase 4 - 04 - ACL du routeur EVA.avi (08:19)

Le routage - phase 4 - 05 - ACL - test et corrections.avi (30:42)

COMPARAISONS DES PROTOCOLES DE ROUTAGE

Source :

<http://www.it-sideways.com/2006/04/rip-igrp-eigrp-ospf-comparison.html>

http://www.certificationzone.com/cisco/newsletter/SL/nla_04-13-04_1.html

<http://threebit.net/mail-archive/cisco-nsp/msg00033.html>

<http://www-lor.int-evry.fr/~vincent/expArad/arad2003/igrp/index.html>

<http://www.juniper.net/techpubs>

<http://www.juniper.net/techpubs/software/junos/>

http://athena.vvsu.ru/docs/CISCO/ito/24_e_igrp_english.htm#HDR13

<http://www.laboratoire-microsoft.org/def/19531/>

PROTOCOLES INTERNES DE ROUTAGE

A VECTEUR DE DISTANCE				A ETAT DE LIENS	
Caractéristiques	RIP v1	IGRP	EIGRP	OSPF	ISIS
Etat de liens				oui	oui
Distance vectorielle	oui	oui	oui		
Résumé de routes automatiques	oui	oui	oui	?	?
Résumé de routes manuelles			oui	?	?
Support VLSM (variables-length sous- réseaux)			oui	oui	oui
protocoles propriétaires		oui	oui		oui
Temps de convergence	lent	lent	très rapide	très rapide	très rapide

PROTOCOLES INTERNES DE ROUTAGE

A état de liens		A vecteur de distance	
OSPF = Open Shortest Path First (protocole non propriétaire) (métrique : la détermination du chemin, la commutation.)		RIP = Routing Information Protocol (métrique : le nombre de sauts)	
IS-IS = Integrated Intermediate System to Intermediate System (protocoles propriétaire) (métrique : la détermination du chemin, la commutation.)		IGRP = Interior Gateway Routing Protocol (protocoles propriétaire CISCO) (métrique : délai d'interréseau, bande passante, fiabilité, charge)	
	EIGRP = Enhanced Interior Gateway Routing Protocol (hybride Etats de lien / a vecteur de distance)		
Inconvénients	Avantages	Inconvénients	Avantages
	Création de la topologie exacte du réseau car :		Détermine la direction et la distance jusqu'à une liaison quelconque de l'inter-réseau.
Chaque fois qu'un paquet de mise à jour de routage à état de liens entraîne une modification dans la base de données d'état de liens, l'algorithme du plus court chemin d'abord recalcule les meilleurs chemins et met à jour la table de routage. (inconvénient car : Surcharge du système + Mémoire requise + Consommation de bande passante).	Base de données topologique : Une base de données topologique est un ensemble d'informations rassemblées à partir des mises à jour de routage à état de liens.	ne permet pas à un routeur de connaître la topologie exacte d'un inter-réseau, étant donné que chaque routeur voit uniquement ses voisins.	L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau.
	Algorithme SPF – L'algorithme du plus court chemin d'abord (SPF) est un calcul effectué sur la base de données qui génère un arbre SPF.		Chaque entrée de la table de routage pour chaque réseau correspond à un vecteur de distance cumulé, lequel indique la distance au réseau dans une direction donnée.

	plus rapide, plus précis, plus évolutif que RIP et IGRP. Permet une stabilisation plus rapide après un changement parce qu'il utilise IP directement. permet de calculer plusieurs routes pour chacun des services IP.		
Au début, durant le processus initial de découverte, l'interréseau est submergé et réduit de façon temporaire la bande passante disponible pour le trafic routé des données utilisateur. -->	Par la suite, les protocoles de routage à état de liens ne nécessitent généralement qu'un minimum de bande passante pour envoyer les paquets de mise à jour reflétant les modifications topologiques. L'envoi peut être sporadique ou déclenché par un événement.		

PROTOCOLES INTERNES DE ROUTAGE

		INCONVENIENTS	AVANTAGES
A états de liens	OSPF = Open Shortest Path First (protocole non propriétaire) (métrique : la détermination du chemin, la commutation.)	avantages sur petits réseaux non transmissible à une hiérarchie de domaine avec beaucoup de routeurs.	Supporte la synchronisation LDP-IGP. Soutien CIDR et VLSM. Convergence rapide, développement non propriétaire donc adaptable à beaucoup de routeurs
		Ne transportent pas de routes externes, mais, ... -->	transportent une route par défaut, des routes intra-zone, et des routes interzones.
		Les zones OSPF ne peuvent pas contenir de routeur ASBR et ne supportent pas la configuration de liaisons virtuelles.	
A états de liens	IS-IS = Integrated Intermediate System to Intermediate System (protocoles propriétaire) (métrique : la détermination du chemin, la commutation.)		Convergence rapide dans l'implémentation de l'IOS. Réduction de routes dans l'IGP.
A vecteur de distance	RIP = Routing Information Protocol (métrique : le nombre de sauts)	* ne prend en compte que la distance entre deux machines en termes de saut, mais il ne considère pas l'état de la liaison afin de choisir la meilleure bande passante possible. Ces limitations sont corrigées dans le protocole OSPF. * La limite de nombre de sauts du RIP est de 15, ce qui signifie qu'un réseau qui dépasse 15 sauts successifs ne pourra pas être appris à travers le protocole RIP.	Pour éviter les boucles de routage, le nombre de sauts est limité à 15. Au delà, les paquets sont supprimés.

A vecteur de distance	IGRP = Interior Gateway Routing Protocol (protocoles propriétaire CISCO) (métrique : délai d'interréseau, bande passante, fiabilité, charge)	Moins efficace que OSPF ou ISIS pour les grands réseaux	Configuration facile.
Hybride	EIGRP = Enhanced Interior Gateway Routing Protocol (hybride Etats de lien / a vecteur de distance)	Moins efficace que OSPF ou ISIS pour les grands réseaux	Configuration facile. améliore considérablement les propriétés de convergence et l'efficacité d'exploitation par rapport à l'I.G.R.P. les principaux atouts de l'E.I.G.R.P sont : * Une convergence rapide. * Une utilisation efficace de la bande passante. * La compatibilité avec le V.S.L.M et le C.I.D.R. * La prise en charge des couches réseaux multiples. * L'indépendance par rapport aux protocoles routés.

Wednesday, April 19, 2006

[RIP, IGRP, EIGRP, OSPF comparison](#)

Posted by Brandon Teoh at [1:51 PM](#) _

CCNA Level:

Routing Fundamentals:

- Static Routing: Manually update possible routes.

Dynamic Routing: Only need to update adjacent routes.

Default routing:

- + You can only use default routing on stub networks. It is also useful for summarization of static route.

```
LabC(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.1
```

```
LabC(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.1
```

```
LabC(config)#ip route 192.168.30.0 255.255.255.0 192.168.40.1
```

LabC(config)#ip route 0.0.0.0 0.0.0.0 192.168.40.1 (Just one statement can replace all three above)

Where 192.168.40.1 is known as the gateway of last resort.

Three ways of creating default route.

```
A#ip route 0.0.0.0 0.0.0.0 192.168.40.1 --> A.D = 1
```

```
A#ip route 0.0.0.0 0.0.0.0 s0/0 --> A.D = 0
```

```
A#ip default-network 192.168.40.0 --> REMEMBER to use network ID!
```

When IGP(RIP,IGRP,OSPF) is configured, default-network would be advertised.

Thus, A.D of static route by default = 1 (unless you wish to change it)

Connected interface = 0

static route = 1

EIGRP = 90

IGRP = 100

OSPF = 110

RIP = 120

External EIGRP (AS redistribution) = 170

Unknown = 255 (never be used)

- When routing between routers, layer 3 or above is used.

When the transferring packets between interfaces, layer 2 or below is used.

- Routing from host to router.

ICMP(Layer 3) à IP (Layer 3) à Packet (layer 3) --> ARP (Layer 3) à Frame-Encapsulation(layer 2)
à FCS-CRC (layer 2) à Packet (layer 3).

Router will then do the same thing by pushing the packet into the next interface

- Rule of thumb:

The destination MAC address will always be the router's interface (if you packets are destined for outside the LAN), never hub/bridge/switches.

EIGRP

- Dynamic routing (support very large network)

- classless protocol (subnet mask is preferred to be specified during IP addressing)

- + VLSM (Variable length subnet mask) / CIDR, not by default - seldom asked in the exams

- + Give rise to discontinuous network

- + Auto summarization (forced summarization)

--> Therefore, when advertised for network, you NO need to provide the mask information.

- concept of Autonomous System (share routing information)
- + neighbor discovery
- + Mechanism:
 - + Hello or ACK received
 - + AS numbers match
 - + Identical metrics (K values)
 - + This will create the topology table.
- used only when all routers are Cisco
- hybrid : send distance-vector and link-state packets
 - + distance-vector
 - + Feasible distance = reported distance + metric to the neighbor reporting the route
 - + Reported distance =
 - Event-driven (hold-down value = 0)
 - + suitable for very large networks. (maximum hop count of 255)
- Supported all routed protocols (IP, IPX, AppleTalk)
- + Due to its protocol-dependent modules (PDMs)
- Communication via RTP (Reliable Transport Protocol)
- Reliability is the focus
- uses multi-cast and unicast (when no reply is received from particular router, 16 times max a.k.a reliable multicast).
- Best path selection via DUAL (Diffusing update Algorithm)
 - + Topology table is used as extension to the routing table, for best path analysis. Means that will be used as input towards DUAL algorithm
 - + Fastest routing protocol (a.k.a fastest route convergence)
 - + Each router having a copy of neighbors' routes (neighbor table)
 - + Keep updating the neighbor table
 - Load balance of up to 6 links (based on metrics)
 - + Metrics is refer to link cost (which is then bandwidth and delay by default), however, EIGRP may use a combination of four.(bandwidth, delay, load, reliability)
 - Support "passive interfaces", similar to switch "port-fast"

Others:

- EIGRP routers that belong to different A.S can't share information automatically (they don't become neighbors). This is a good practice to reduce bandwidth.
- If you still insist to share information between these routers, then you have to do it manually. This is known as redistribution.
- Internal EIGRP A.D = 90
- External EIGRP A.D = 170 (when redistribution[automatic or manual] happens)
- + Automatically redistribution - In an existing IGRP network, putting a router with EIGRP having the same A.S as the existing IGRP will bring about automatic redistribution.

- A feasible successor is a backup route and is stored only in the topology table. A successor route is stored in the topology and also the routing table.
Having feasible successor helps with network convergence (thus no need to study the network anymore, just need to update changes)

OSPF:

- Dynamic Routing (large network support)
- classless protocol (subnet mask is preferred to be specified during IP addressing)
- + VLSM/CIDR (not by default)
- + Gives rise to discontinuous network, therefore catering for huge network (reduce bandwidth)
- + Route redistribution - a translation service between routing protocols.

- + No auto-summarization BUT MANUAL summarization.
- > Therefore, when advertised for network, you have to specify the reversed mask. However, you if don't specify the mask information, then it will assume as the default mask.
- Send link-state packets
- Supported only IP routed protocol.
- Minimize routing update traffic (the one with lowest management bandwidth requirement)
- > Because it is event triggered
- Hierarchical network. Because it is using Area (even though everybody has to connect to Area 0). "Area" is actually a subset for Autonomous system (in EIGRP). Typically, OSPF runs inside an autonomous system.
- Topology database is also known as "link-state database". It is used as input to the algorithm for shortest path computation.
- OSPF can work with layer 2 networks of broadcast-multi-access(i.e Ethernet) and Non-broadcast-multi-access(NBMA) (Frame Relay, X.25, ATM), as well as point to point and point to multipoint. BMA, Point to mulitpoint = DR and BDR needed
NBMA, point to point = DR and BDR not needed
- OSPF process ID:
 - + Locally significant only
 - + Grouping of commands under specific running process. (Each process maintain separate copy of its topology table)
 - + Enable OSPF routing on the router.
- Recommended to use loopback interfaces because it will always be active, and since loopback interfaces' IP will become the router ID, this will also affect selection for DR and BDR.

RIPv2:

- classless protocol
- Auto-summarization (forced summarization)
- > Therefore, when advertised for network, NO need to specify the netmask.
- Supported only IP routed protocol.
- Distance-vector protocol
- Gives rise to pinhole congestion
- Slow convergence time.
- + Gives rise to inconsistent routing tables and routing loops (when update not done simultaneously).
- Routing loop counter mechanism:
 - + Split horizon = never send back to same direction
 - + Route poisoning = set the hop count in routing table to 16

Routing loop counter tool:

- + Holddowns timer
- + Maximum hop count =15 (the number 15 is considered as a loop)
- > Split horizon and route poisoning rely on holddowns timer and maximum hop count for its working. --> Exam question
- + Not suitable for large network.

RIPv1:

- classfull protocol
- + No VLSM
- Auto-summarization (forced summarization)
- > Therefore, when advertised for network, NO need to specify the netmask.
- Supported only IP routed protocol
- Load balance of up to four links (with equal cost links, that is hop count.)

- Distance-vector protocol
 - Gives rise to pinhole congestion
 - Slow convergence time.
 - + Gives rise to inconsistent routing tables and routing loops (when update not done simultaneously).
- Routing loop counter mechanism:
- + Split horizon = never send back to same direction
 - + Route poisoning = set the hop count in routing table to 16

Routing loop counter tool:

- + Holddowns timer
- + Maximum hop count = 15 (the number 15 is considered as a loop)
- > Split horizon and route poisoning rely on holddowns timer and maximum hop count for its working. --> Exam question
- + Not suitable for large network.

IGRP

- classfull protocol
- + No VLSM
- Supported only IP routed protocol
- Distance-vector protocol
- Maximum hop count of 255, however uses bandwidth and delay as the metric instead.

All in one:

- RIPv2 and EIGRP support discontinuous networking, but not by default. OSPF does support discontinuous networking by default because it does not auto summarize classful boundaries as RIP and IGRP do.
- By default, RIP can load balance across four links as well. However, unlike IGRP and EIGRP, they must be equal links (hop count)
- Under RIP, the passive-interface command will prohibit the sending of route updates but allow their receipt. Thus, a RIP router with a passive interface will still learn about the networks advertised by other routers. This is different from EIGRP, where a passive-interface will neither send nor receive updates.
- Multi vendors environment --> RIPv1 (outdated), RIPv2 (smaller network), OSPF (large network)
- Cisco only --> IGRP(outdated), EIGRP (large network)
- Static route between two ends has the less bandwidth requirement.
- Link-state protocol has more intelligence than distance-vector protocol. Hybrid is the king.
- RIP & IGRP can only be used on a classful network (with consistent subnet masks)

Tips:

- Always compare OSPF to RIPv2 and RIPv1 because these are open-standard. Thus, within an all cisco-router environment, EIGRP would be the best choice.
- Due to slow convergence nature, RIPv1 and RIPv2 requires too much bandwidth, thus OSPF is preferred.
- classfull protocol means either:
 1. Don't think about subnet / ignore subnet
 2. Use the most significant octets

For instance: the classful of 172.16.0.0 /24 is 172.16.0.0
not 172.16.10.0

LE PROTOCOLE OSPF

Le protocole OSPF :

<http://netcenter.cumt.edu.cn/network/wlzs/ospf/configospf.pdf>

<http://www.juniper.net/techpubs/software/erx/erx50x/swconfig-routing-vol1/html/ospf-config8.html>

<http://www.linux-france.org/prj/edu/archinet/systeme/ch68.html>

Adressage IP et configuration des routeurs

Aide à la configuration des routeurs :

<http://www.nskb.net>

Adressage IP - Explications :

<http://www.commentcamarche.net/internet/ip.php3>

<http://www.vulgarisation-informatique.com/masque-sous-reseau.php>

<http://www.commentcamarche.net/forum/affich-1947253-calcul-masque-reseau>

Les commentaires des videos :

ERRATUM durant les videos ! Surligange ici et correction en rouge

Le routage - phase 1 - Choix du protocole de routage.txt

Afin de finir les annotations et commencer la configuration, il faut allumer les éléments.

* Nous remarquons que certaines connections ont des point verts : ce qui signifie un branchement correct ne nécessitant aucune configuration spécifique.

* par contre, celles avec les points rouges sont à configurer.

Nommons maintenant les éléments.

Afin de bien configurer les différents éléments, déterminons dans un premier temps le type d'adresses réseaux ou plutôt quelles classes nous allons utiliser.

adresse réseau : réseau privé donc adressage privé = classe A (10.0.0.0 à 10.255.255.255)

ou classe B (172.16.0.0 à 172.31.255.255)

ou classe C (192.168.0.0 à 192.168.255.255)

Une adresse IP de classe C dispose de trois octets pour identifier le réseau et d'un seul octet pour identifier les machines sur ce réseau. Ainsi, un réseau de classe C peut comporter jusqu'à 254 postes, soit 254 terminaux. Ce qui suffisant dans cette configuration.

Nombres de sous-réseaux nécessaires : 5

Déterminons visuellement les sous réseaux.

Les 5 surfaces de couleurs différentes montrent le nombre de réseaux nécessaires.

Déterminons le protocole de routage : ...

CE QUE NOUS SAVONS :

Il existe des protocoles de routage interne et Externe. Ici, nous avons besoin d'un protocole interne.

Les IGP sont des protocoles fonctionnant à l'intérieur d'un système autonome.

Ces protocoles de routage interne fonctionnent de différentes façons :

* Protocoles de routage à états de lien :

OSPF = Open Shortest Path First

IS-IS = Integrated Intermediate System to Intermediate System

* Protocoles de routage à vecteur de distance :

RIP = Routing Information Protocol

IGRP = Interior Gateway Routing Protocol

* Protocoles hybride des deux premiers :

EIGRP = Enhanced Interior Gateway Routing Protocol

A première vue, chacun des cinq protocoles pourraient convenir. Etudions les avantages et inconvénients de chacun.

Comparaison des avantages et inconvénients des protocoles internes :

Procédons par élimination :

- déterminons quel protocole a états de liens nous retiendrions.
- déterminons quel protocole a vecteurs de distance nous retiendrions.(y compris le protocole Hybride EIGRP)

Pour cela, je m'aide des données que j'ai rassemblées sur INTERNET.

il s'agit de la formation CISCO, d'une présentation powerpoint de chez JUNIPER (un fabricant de routeur) et de diverses sources (laboratoire-microsoft.org, supinfo.com, Wikipedia.com, données universitaires françaises, ...)

et Un article comparant les différents protocoles, d'après Brandon Teoh.

Après lecture approfondis des comparatifs, retenons OSPF.

(EIGRP serait aussi un bon choix. Nous l'utiliserons d'ailleurs si Packet tracer 5.0 ne gère pas l'OSPF et si ce dernier est trop complexe à mettre en œuvre)

Le routage - phase 2 - 001 à 002 - Choix du réseau.txt

Pour permettre une meilleure insertion de notes, nous remettons en forme le schéma.

Pour insérer une note, utiliser l'icone sur la droite.

1) Création du sous-réseau :

Au niveau de cette phase 2, nous avons 5 sous-réseaux avec au maximum de 2 stations de travail par routeur.

un adressage de classe C, avec une plage d'adresse de sous-réseau offrant 254 postes de travail est largement suffisant.

par exemple, une plage de classe d'adresses C de réseau 192.168.222.1 à 192.168.222.254 conviendrait.

EXPLICATIONS :

la classe C correspond aux adresses du réseau 192.168.0.0, c'est-à-dire les adresses (la plage d'adresses utilisable) de réseau 192.168.0.1 à 223.255.255.254

(La première adresse d'un réseau spécifie le réseau lui-même, la dernière est une adresse de diffusion (broadcast)).

(Exemple ici : adresse du réseau correspond à 192.168.0.0 et l'adresse de diffusion est 223.255.255.255)

(ne pas confondre : "adresses du réseau ..." et "adresses de réseau ... à ...")

Cependant, ici, nous avons besoin d'un adressage privé.

la classe C correspondant aux adresses privées du réseau s'étant de 192.168.0.1 à 192.168.0.254

Ce qui laisse $2^8 - 2^0 = 255$ réseaux avec 254 Stations de travail disponibles par réseau.

Dans notre cas, il n'y a besoin que de UN réseau dans l'entreprise donc nous choisissons UNE plage parmi les 255 disponible.

par exemple : 192.168.222.1 à 192.168.222.254

2) création du masque de sous-réseau :

Notre plage de classe d'adresses C, 192.168.222.1 à 192.168.222.254 a besoin d'un masque pour le filtrage des adresses.

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. le quatrième étant pour les hôtes.

(exemple : 192.168.0.0 s'écrit aussi 11000000.10101000.00000000.00000000

192.168.255.255 s'écrit aussi 11000000.10101000.11111111.11111111)

Le nombre de sous-réseaux dépend du nombre de bits attribués en plus au réseau.

c'est-à-dire, qu'une partie des bits de l'octet réservé aux hôtes est utilisé pour définir le nombre de sous-réseaux.

Nombre de bits	Nombre de sous-réseaux
1	2
2	4
3	8
4	16
5	32
6	64

dans notre cas, nous avons besoin de 5 sous-réseaux, donc nous devons réserver une adresse de classe c avec un minimum de 3 bits sur le 4ème octet.

Prenons donc 192.168.222.1 (notation décimale)
11111111.11111111.11011110.00000001 (notation binaire)

Le masque à appliquer sera alors :

255 .255 .255 .224 (notation décimale)
11111111.11111111.11111111.11100000 (notation binaire)

d'où :

11111111.11111111.11011110.00000001
ET 11111111.11111111.11111111.11100000 (noté aussi /27 car il y a 27 bits pour le découpage du réseau en sous-réseaux)
= 11111111.11111111.11111111.00000000 (soit 192.168.222.0)

En réalité, il y a donc 8 plages possibles pour le résultat du masquage de cette adresse IP :

- * Soit les 3 premiers bits du 4ème octet sont 000, auquel cas le résultat du masquage est 192.168.222.0
- * Soit les 3 premiers bits du 4ème octet sont 001, auquel cas le résultat du masquage est 192.168.222.32
- * Soit les 3 premiers bits du 4ème octet sont 010, auquel cas le résultat du masquage est 192.168.222.64
- * Soit les 3 premiers bits du 4ème octet sont 011, auquel cas le résultat du masquage est 192.168.222.96
- * Soit les 3 premiers bits du 4ème octet sont 100, auquel cas le résultat du masquage est 192.168.222.128
- * Soit les 3 premiers bits du 4ème octet sont 101, auquel cas le résultat du masquage est 192.168.222.160
- * Soit les 3 premiers bits du 4ème octet sont 110, auquel cas le résultat du masquage est 192.168.222.192
- * Soit les 3 premiers bits du 4ème octet sont 111, auquel cas le résultat du masquage est 192.168.222.224

* Soit les 3 premiers bits du 4ème octet sont 111, auquel cas le résultat du masquage est 192.168.222.255

En conclusion:

Nous avons donc un réseau d'adresse IP de 192.168.222.0/27

nous avons le choix entre 8 plages d'adresses de sous-réseau pour les 5 sous-réseaux nécessaires.

SOURCES :

yannick.kohler@afpa.fr

CISCO CCNA 1 + 1

<http://www.commentcamarche.net/internet/ip.php3>

<http://www.vulgarisation-informatique.com/masque-sous-reseau.php>

<http://www.commentcamarche.net/forum/affich-1947253-calcul-masque-reseau>

Le routage - phase 2 - 003 - répartition adresses IP.txt

REPARTITION DE : ADRESSES IP / ADRESSES IP passerelles / SOUS-RESEAU / MASQUE :

Nous avons choisi 192.168.222.0 en adresse du réseau.

Pour la notation, partons par exemple du routeur CENTER et choisissons les 5 sous-réseaux parmi les 8 possibles :

Nous avons choisi les plages 1 à 5 comprises parmi les 8 plages utilisables d'adresses de réseau :

Nous avons choisi les plages **1, 2, 3, 5 et 6** comprises parmi les 8 plages utilisables d'adresses de réseau :

plage 1 : 192.168.222.1/27 à 192.168.222.30/27 (avec adresse du sous-réseau 192.168.222.0 et adresse de diffusion 192.168.222.31)

plage 2 : 192.168.222.33/27 à 192.168.222.62/27 (avec adresse du sous-réseau 192.168.222.32 et adresse de diffusion 192.168.222.63)

plage 3 : 192.168.222.65/27 à 192.168.222.94/27 (avec adresse du sous-réseau 192.168.222.64 et adresse de diffusion 192.168.222.95)

plage 4 : 192.168.222.97/27 à 192.168.222.126/27 (avec adresse du sous-réseau 192.168.222.96 et adresse de diffusion 192.168.222.127)

plage 5 : 192.168.222.129/27 à 192.168.222.158/27 (avec adresse du sous-réseau 192.168.222.128 et adresse de diffusion 192.168.222.159)

plage 6 : 192.168.222.161/27 à 192.168.222.190/27 (avec adresse du sous-réseau 192.168.222.160 et adresse de diffusion 192.168.222.191)

plage 7 : 192.168.222.193/27 à 192.168.222.222/27 (avec adresse du sous-réseau 192.168.222.192 et adresse de diffusion 192.168.222.223)

plage 8 : 192.168.222.225/27 à 192.168.222.254/27 (avec adresse du sous-réseau 192.168.222.224 et adresse de diffusion 192.168.222.255)

1) "ETAGE 1" : Nous partons du routeur CENTER, puis nous élargissons l'arborescence adjacente a chaque "étage de routeur"

CONNEXION N°1 adjacente DU ROUTEUR CENTER :

Interface du routeur CENTER : Fast Ethernet 0/0

Adresse IP Routeur CENTER : 192.168.222.1

CONNEXION N°2 adjacente DU ROUTEUR CENTER :

Interface du routeur CENTER : SERIAL 0/0 DCE

Adresse IP Routeur CENTER : 192.168.222.33

CONNEXION N°3 adjacente DU ROUTEUR CENTER :

Interface du routeur CENTER : SERIAL 0/1 DCE

Adresse IP Routeur CENTER : 192.168.222.65

CONNEXION N°2 DU ROUTEUR CENTER au routeur BOAZ :

Interface du routeur CENTER : Serial 0/0 DCE

Adresse IP Routeur CENTER : 192.168.222.33

Interface du routeur BOAZ : Serial 0/0 DTE

Adresse IP Routeur BOAZ : 192.168.222.34

CONNEXION N°3 DU ROUTEUR CENTER au routeur EVA :

Interface du routeur : SERIAL DCE 0/1

Adresse IP Routeur CENTER : 192.168.222.65

Interface du routeur : SERIAL 0/1 DTE

Adresse IP Routeur EVA : 192.168.222.66

Commentaires :

lorsque deux routeurs adjacents sont connectés sur le port série, l'un est en DCE, et l'autre est en DTE

Pour relier deux routeurs directement, il faut utiliser le port série (ex : SERIAL 0/0)

Par simplicité, la numérotation du dernier octet se suit au fur et à mesure de l'avancement du réseau, d'une station de travail à l'autre.

2) "ETAGE 2" :

CONNEXION DU ROUTEUR BOAZ a la suite du sous-réseau (1ère partie):

Interface du routeur : Fast Ethernet 0/0

Adresse IP Routeur BOAZ : 192.168.222.129

CONNEXION DU ROUTEUR EVA a la suite du sous-réseau (1ère partie) :

Interface du routeur : Fast Ethernet 0/1

Adresse IP Routeur CENTER : 192.168.222.161

Commentaires :

Pour relier un routeur directement au switch, il faut utiliser le port Fast Ethernet (ex : Fast Ethernet 0/0)

Par simplicité, la numérotation du dernier octet se suit au fur et à mesure de l'avancement du réseau, d'une station de travail à l'autre.

3) CONNEXION N° 1 DU ROUTEUR CENTER à la suite du sous-réseau :

SERVEUR N°1

Adresse du serveur 1 : 192.168.222.11
passerelle par défaut : 192.168.222.1
Nombre de sous-réseaux : 5
Masque de sous-réseau : 255.255.255.224

Station de travail n°2

Adresse IP de la station de travail 2 : 192.168.222.12
passerelle par défaut : 192.168.222.1

Pour le serveur N°1 et la station de travail N°2, l'adresse IP de la passerelle et celle de la connexion au routeur direct.

De la même manière, nous noterons les autres connexions entre les stations de travail et leur routeur respectif.

4) CONNEXION DU ROUTEUR BOAZ à la suite du sous-réseau (2ème partie) :

Interface du routeur : Fast Ethernet 0/0
Adresse IP Routeur BOAZ : 192.168.222.129

Adresse IP de la station de travail 3 : 192.168.222.130
passerelle par défaut : 192.168.222.129

Adresse IP de la station de travail 4 : 192.168.222.131
passerelle par défaut : 192.168.222.129

5) CONNEXION DU ROUTEUR EVA à la suite du sous-réseau (2ème partie) :

Interface du routeur : Fast Ethernet 0/1
Adresse IP Routeur EVA : 192.168.222.161

Adresse IP de la station de travail 5 : 192.168.222.162
passerelle par défaut : 192.168.222.161

Adresse IP de la station de travail 6 : 192.168.222.163
passerelle par défaut : 192.168.222.161

Merci de votre attention :

Le routage - phase 2 - 004 - configuration des éléments.txt

CONFIGURATION DES DIFFERENTS ELEMENTS DU RESEAU :

1) Le serveur N°1 :

??? notes non sauvegardées !

Le routage - phase 2 - 005 - test éléments (sans routeur).txt

CONFIGURATION DES DIFFERENTS ELEMENTS DU RESEAU :

Comme rien n'a été testé auparavant, il est fort probable que je fasse des erreurs, désolé ;)
Elles seront corrigées au fur et à mesure des essais, mais pas de vidéos des corrections !

- 1) Le serveur N°1
- 2) les stations de travail
- 3) Le Switch : pour le moment rien
- 4) les routeurs ... vidéos suivantes

Exemple d'une vérification de configuration correcte entre le serveur 1 et la station de travail 2 :
Deux manières de faire :

- test automatique en sélectionnant les deux éléments qui doivent communiquer
- test manuel en configurant a qui est envoyé le paquet

Ceci est valable entre tout type d'élément

Si la connexion est établie correctement, nous avons la confirmation "successful", Sinon "failed"

Dans ce cas, c'est normal, car les routeurs ne sont pas encore configurés.

Dans cet autre cas, c'est qu'une des stations de travail est mal configurée. Corrigeons l'erreur.

Le routage - phase 2 - 006 - suppression câblage routeurs par défaut.txt

CONFIGURATION DES ROUTEURS :

Nous avons besoin sur les routeurs de 2 ports série et de 2 ports Fast Ethernet (même si tous ne sont pas utilisés)

Cela ne peut se faire que si le routeur est éteint.

depuis le début, les routeurs ont déjà des connexions placés automatiquement mais non configurées.

Ceci a été fait juste pour montrer le schéma dans son ensemble

Enlevons toutes les connexions des routeurs et mettons celles qui seraient appropriées

Le routage - phase 2 - 007 - connexions routeur et cablage.txt

CONFIGURATION DES ROUTEURS :

Nous avons besoin sur les routeurs de 2 ports serie et de 2 ports Fast Ethernet (même si tous ne sont pas utilisés)

Cela ne peut se faire que si le routeur est éteint.

plaçons les bonnes interfaces et connexions entre les routeurs et le reste des éléments.

Deux possibilités pour les connexions :

- soit automatique
- soit en choisissant manuellement

Il est possible que la connectique entre les routeurs soit aussi serial DCE avec une horloge (clock rate).

Le routage - phase 2 - 008 - ajustement connexions routeur et cablage.txt

CONFIGURATION DES ROUTEURS :

En fonction de ce que nous avons choisi comme interface lors de la connexion au routeur, nous allons ajuster les annotations.

En plaçant (et en attendant 2 seconde) le curseur sur symbole (un rond) schématisant la connexion, nous voyons apparaitre le nom de l'interface connecté.

exemples :

SER 0/0 pour l'interface SERIAL 0

SER 1/0 pour l'interface SERIAL 0

Fa 2/0 pour l'interface Fast Ethernet 2

Le numéro de gauche correspond à l'ordre d'enchâssement de la carte périphérique (série, fast Ethernet, ...) de droite à gauche dans le routeur.

Le routage - phase 2 - 009 - Correction du nom des éléments.txt

CONFIGURATION DES ROUTEURS : Correction du nom des éléments.

Lors de la configuration des adresses IP des hôtes ou des interfaces sur les routeurs (nous verrons cela bien après), il ne faut pas que les noms des éléments comportent des espaces :

ex : "Station de travail N°2" est renommé en "station_de_travail_2"

Le routage - phase 3 - 010 - IOS Command line center - mot de passe.txt

CONFIGURATION DES ROUTEURS : IOS Command line Interface

Nous allons commencer comme-ci nous n'avions jamais configuré ces routeurs.

1.) Configuration du nom du routeur et des mots de passe.

Nous allons commencer par nommer les routeurs, selon les noms indiqués sur le schéma topologique.

Rappel : un routeur peut fonctionner sous trois modes (niveaux d'accès) : mode utilisateur (commandes non destructives), privilégié (examen plus approfondi du routeur) et le mode configuration (jeu de commandes complet pour la configuration du routeur). Pour configurer le nom et les mots de passe du routeur, nous devons donc entrer en mode de configuration

La commande "enable" permet de passer en mode privilégié,

La commande "configure terminal" ou "conf t" permet de passer en mode de configuration globale.

La commande "hostname nom_de_routeur" permet de définir le nom du routeur

On peut voir désormais que le nom a changé dans la ligne commande

Configuration des mots de passe :

Il existe plusieurs mots de passe sur un routeur :

- le mot de passe Utilisateur (mot de passe console)

- le mot de passe pour rentrer en mode privilégié

- le(s) mot(s) de passe pour les sessions Telnet

 - (ces sessions vous permettent de configurer un routeur distant).

Cette commande définit le mot de passe « sec_center » comme mot de passe pour rentrer dans le mode privilégié.

La sécurisation du routeur grâce aux mots de passe est importante. Mieux vaut le faire dès le début.

A partir du mode configuration globale, nous devons passer en mode de configuration de la console (la console étant le périphérique)

"Line console 0" nous fait donc passer dans ce mode.

"Login" indique au routeur que vous désirez mettre en place l'authentification des utilisateurs du routeur.

"Password mot_de_passe" indique le mot de passe.

Ainsi, au démarrage du routeur nous avons pour le moment ceci :

User Access Verification

Password: cons_center

CENTER>enable

Password: sec_center
CENTER#

La dernière étape concernant les mots de passe concerne les mots de passe pour les sessions Telnet. Si l'on ne configure pas ces mots de passe, les sessions Telnet ne peuvent, pour des raisons de sécurité évidentes, avoir lieu.

Pour définir ces mots de passe, nous devons passer en mode configuration de terminal virtuel.

"Line console vty 0 4" signifie que l'on veut configurer les 5 terminaux virtuels en même temps (du terminal 0 au terminal 4). En effet, il ne peut y avoir plus de 5 sessions telnet en même temps.

par contre, bien penser à sauver la configuration courante :

```
CENTER#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CENTER#
```

De la même manière que pour le routeur CENTER, nous configurons pour le moment les routeurs BOAZ et EVA.

Routeur Boaz : configuration

Routeur Eva : configuration

2.) Configuration des interfaces des routeurs :

2.1) Routeur CENTER

(A noter que les mots de passe n'apparaissent jamais !)

Interface fastEthernet 2/0 => commande permettant de passer en mode de configuration d'interface

ip address adresse_ip masque_de_sous-réseau => commande pour définir l'adresse

no shutdown => commande d'indiquant au routeur que cette interface doit toujours rester ouverte

De la même manière, configurons les interfaces séries

exit => commande permettant de revenir au mode précédent

conf t => commande permettant de passer en mode de configuration terminal (si depuis le début)

int s0 => commande permettant de passer en mode de configuration d'interface série (ici interface série 0)

clockrate => commande définissant la fréquence d'horloge des connexions matérielles

Seule l'interface ETCD (DCE en anglais) peut avoir un clockrate de défini.

De la même manière, configurons les interfaces séries

Interface série DCE 1/0

exit => commande permettant de revenir au mode précédent
conf t => commande permettant de passer en mode de configuration terminal (si depuis le début)

int s0 => commande permettant de passer en mode de configuration d'interface série (ici interface série 1)

clockrate => commande définissant la fréquence d'horloge des connexions matérielles
Seule l'interface ETCD (DCE en anglais) peut avoir un clockrate de défini.

De la même manière, configurons les interfaces type fast Ethernet du routeur Boaz
Interface fast Ethernet 2 (interface fast Ethernet 2/0)

De la même manière, configurons les interfaces type serie du routeur Boaz
Interface serie 0/0 (int s0/0)

De la même manière, configurons les interfaces type fast Ethernet du routeur EVA
Interface fast Ethernet 2 (interface fast Ethernet 2/0)

De la même manière, configurons les interfaces type serie du routeur EVA
Interface serie 0/0 (int s0/0)

CONFIGURATION DES ROUTEURS : IOS Command line Interface

3.) Configuration des réseaux

3.1) Routeur CENTER

3.2) Routeur BOAZ

3.3) Routeur EVA

CENTER(config)#routeur OSPF 1

=> le "1" définit le cout par défaut (1 pour l'Ethernet supérieur à 100 Mbps). OSPF privilégie les routes qui ont un coût faible, donc celles qui sont supposées rapides en terme de débit théorique.

CENTER(config-router)#Network 192.168.222.0 0.0.0.255 area 222

=> "network" pour la configuration réseau ... donc il faut une adresse RESEAU. ex ici :
192.168.222.0

=> "192.168.222.0" est l'adresse du réseau avec "0.0.0.255" comme masque générique

=> "area 222" définit la zone de réseau 222. Il y a un numéro de zone par réseau.

procédons de même pour les routeurs BOAZ et EVA

CONFIGURATION DES ROUTEURS : IOS Command line Interface

4.) Configuration des hôtes : Routeur CENTER puis Routeur BOAZ puis Routeur EVA

l'adresse indiquée après le nom du routeur doit être celle de l'interface depuis laquelle l'information provient.

Cependant, ici, le réseaux est tout petit. Nous pouvons nous permettre pour des raisons de facilité d'avoir une même configuration de table d'hôtes pour les trois routeurs.

CENTER(config)#ip host BOAZ 192.168.222.34

=> Information provenant du routeur Boaz depuis l'adresse 192.138.222.34 (port série S0/0)

CONFIGURATION DES ROUTEURS : IOS Command line Interface

Phase de test : notons les erreurs !

A priori, il y a une mauvaise configuration sur le routeur EVA ! C'est résolu :)

Merci de votre Attention !

CONFIGURATION DES ROUTEURS : IOS Command line Interface

6.) insertion d'une bannière : AUTHORIZED ACCES ONLY

En mode de configuration terminal : commande : banner motd 'le texte a rentrer'

Le routage - phase 4 - 012 - listes de contrôle d'accès.txt

PHASE 4 : LES LISTES DE CONTROLE D'ACCES (ACL = Access Control List) :

Après lecture de la documentation, nous pouvons établir la démarche de création des Listes de contrôle d'accès.

Voici la politique des listes d'accès (ACL) utilisée ici :

Nous prendrons de préférence des ACL nommées. La gestion se fera au plus proche de la source (souvent sur les interfaces d'entrées des équipements hôtes vers le routeur).

Les ACL nommées permettent une plus grande souplesse lors de modifications du réseau.

Mais, cette version de packet tracer 5.0 ne permet pas d'utiliser correctement les noms.

Nous utiliserons donc simplement des ACL étendues (avec des numéros seulement)

Exemple ACL standard :

```
Router(config)#access-list access-list-number {deny | permit | remark} source [source-wildcard]
[log]
```

```
Router(config)#access-list 123 deny host 192.168.222.26 host 192.168.222.120
```

Exemple ACL standard nommée : Router(config)#ip access-list standard eva

Exemple ACL étendue : Router(config)#ip access-list extended 123

Exemple ACL étendue nommée : Router(config)#ip access-list extended eva

Méthode :

- 1.) A la source du routeur, noter en face de chaque interface ce qui doit être bloqué avec les autorisations spécifiques.
- 2.) De même, noter ce qui est autorisé avec les autorisations spécifiques.

En bilan après lecture :

- tous les routeurs ont permission d'accès sur tout équipement.
- "serveur 1" et "station de travail 2" ont permission d'accès sur tout équipement.
- le "sous-réseau Boaz" et le "sous-réseau Eva" ont permission d'accès seulement sur leur sous-réseau respectif
- cependant:

"station de travail 3" peut accéder (requête de ping uniquement) à "station de travail 6"
"station de travail 4" ne peut pas accéder à "routeur EVA" en connexion Telnet

ATTENTION :

* Une requête de ping est différent d'une connexion. La requête de ping à un caractère "unidirectionnel", dans le sens ou il n'y a pas connexion "birectionnelle".

* Il est important de savoir que, implicitement, à la fin d'une liste de contrôle d'accès, l'instruction "deny ip any any" existe. Ce qui a pour effet de refuser toute connexion ne répondant pas aux exigences des lignes d'instructions précédentes. il est intéressant de donner un caractère explicite en écrivant cette instruction en fin de liste.

Démarche générale :

- 1) connexion au routeur
- 2) passage en mode de configuration terminal : "conf t"
- 3) passage mode de configuration étendue (création de l'ACL) : "ip access-list extended numéro_de_liste"
- 3) instructions de l'ACL (particulier vers le plus général) : "permit ip host @ip_source host @ip_destination"
- 4) passage en mode de configuration d'interface : "interface fastethernet numéro_interface"
- 5) liaison de la liste de contrôle d'accès étendue existante à l' interface : "ip access-group numéro__liste {in | out}"
- 6) sauvegarder : "copy running-config startup-config"

ACL du routeur CENTER :

- * il n'y a pas besoin d'ACL sur ce routeur car toutes les informations traversent.
- * de plus se sont des ACL étendues et le sous réseau 192.168.222.0 n'a pas de restrictions.

ACL du routeur BOAZ :

- * permettre la requête de ping du routeur BOAZ vers le sous-réseau BOAZ (stations de travail 3 à 4)
 - => requête de ping : mettre "ICMP" comme protocole au début de l'instruction
 - => @ du sous-réseau Boaz : 192.168.222.128
 - => masque générique : 0.0.0.31 (255 - "dernier octet masque de sous-réseau" = 255-224 = 31)
 - => @ de l'interface FastEthernet 2/0 (vu comme un hôte => host) du routeur Boaz : 192.168.222.129
 - => requête de ping : mettre "echo-reply" à la fin de l'instruction pour éviter une connexion bidirectionnelle

- * permettre la requête de ping du routeur CENTER vers le sous-réseau BOAZ (stations de travail 3 à 4)
- * permettre la requête de ping du routeur EVA vers le sous-réseau BOAZ (stations de travail 3 à 4)
- * permettre la connexion du sous-réseau BOAZ (stations de travail 3 à 4) au serveur_1

- * permettre la requête de ping de "station de travail 2" vers sous-réseau du routeur BOAZ (stations de travail 3 à 4)

- * permettre la requête de ping de "station de travail 3" vers "station de travail 6" (appartient au sous-réseau EVA)

- * normalement : "echo-reply" enfin d'instruction pour une simple requête de ping

- * mais inutile ici car "echo-reply" sera placé sur une instruction du routeur EVA

- * de plus, sur ce sous-reseau 192.168.222.128, "station de travail 3" peut avoir une connexion complète vers vers "station de travail 6"

- * fin des instructions de l'ACL numérotée 128 appliquée au routeur BOAZ

- * paramétrage explicite de l'instruction "deny ip any any"

4) passage en mode de configuration d'interface : "interface fastethernet numéro_interface"

5) liaison de la liste de contrôle d'accès étendue existante à l' interface : "ip access-group numéro__liste {in | out}"

6) sauvegarder : "copy running-config startup-config"

fin !

ACL du routeur EVA :

- * permettre la requête de ping du routeur EVA vers le sous-réseau EVA (stations de travail 5 à 6)

- => requête de ping : mettre "ICMP" comme protocole au début de l'instruction

- => @ du sous-réseau EVA : 192.168.222.160

- => masque générique : 0.0.0.31 (255 - "dernier octet masque de sous-reseau" = 255-224 = 31)

- => @ de l'interface FastEthernet 2/0 (vu comme un hôte => host) du routeur EVA :

192.168.222.129

- => requête de ping : mettre "echo-reply" à la fin de l'instruction pour éviter une connexion bidirectionnelle

- * permettre la requête de ping du routeur CENTER vers le sous-reseau EVA (stations de travail 5 à 6)

- * permettre la requête de ping du routeur BOAZ vers le sous-reseau EVA (stations de travail 5 à 6)

- * permettre la connexion du sous-reseau EVA (stations de travail 5 à 6) au serveur_1

- * permettre la requête de ping de "station de travail 2" vers "sous-réseau du routeur EVA (stations de travail 5 à 6)"

- * permettre la requête de ping de "station de travail 3" vers "station de travail 6" (appartient au sous-réseau EVA)

- * "echo-reply" enfin d'instruction pour une simple requête de ping

- * fin des instructions de l'ACL numérotée 160 appliquée au routeur EVA

* paramétrage explicite de l'instruction "deny ip any any"

4) passage en mode de configuration d'interface : "interface fastethernet numéro_interface"

5) liaison de la liste de contrôle d'accès étendue existante à l'interface : "ip access-group numéro__liste {in | out}"

6) sauvegarder : "copy running-config startup-config"

fin !

PHASE 4 : LES LISTES DE CONTROLE D'ACCES (ACL = Access Control List) : TEST

Par défaut, ce qui n'est pas précisé comme "autorisé" est donc "bloqué"

La station de travail 2 et le serveur de fichiers 1 se trouvent sur le réseau de gestion. N'importe quelle unité du réseau de gestion peut accéder à n'importe quel équipement sur l'ensemble du réseau.

Les stations de travail connectées aux LAN Eva et Boaz ne sont pas autorisées en dehors de leur sous-réseau, sauf pour accéder au serveur de fichiers 1.

Chaque routeur peut envoyer une requête telnet aux autres routeurs et accéder à n'importe quelle unité sur le réseau.

=> CORRECTION !!!! : no permit ip afin de retirer la mauvaise instruction !

Remplacement par la bonne instruction.

=> RE-CORRECTION : il faut déplacer l'instruction "deny ip any any" ! Quel évidence ! et la replacer en fin

Vérifications plus spécifiques :

Connexion TELNET de Boaz à Eva RÉUSSIE

Connexion TELNET de la station de travail 4 à Eva BLOQUÉE

Connexion TELNET de la station de travail 5 à Boaz BLOQUÉE

Connexion TELNET de la station de travail 2 à Boaz RÉUSSIE

Connexion TELNET de la station de travail 2 à EVA RÉUSSIE

Requête ping de la station de travail 5 vers le serveur de fichiers 1 RÉUSSIE

Requête ping de la station de travail 3 vers le serveur de fichiers 1 RÉUSSIE

Requête ping de la station de travail 3 vers la station de travail 4 RÉUSSIE

La station de travail 2 et le serveur de fichiers 1 se trouvent sur le réseau de gestion. N'importe quelle unité du réseau de gestion peut accéder à n'importe quel équipement sur l'ensemble du réseau.

Les stations de travail connectées aux LAN Eva et Boaz ne sont pas autorisées en dehors de leur sous-réseau, sauf pour accéder au serveur de fichiers 1.

Chaque routeur peut envoyer une requête telnet aux autres routeurs et accéder à n'importe quelle unité sur le réseau.

Vérification plus spécifique :

Connexion TELNET de Boaz à Eva	RÉUSSIE	
Connexion TELNET de la station de travail 4 à Eva	BLOQUÉE	
Connexion TELNET de la station de travail 5 à Boaz	BLOQUÉE	
Connexion TELNET de la station de travail 2 à Boaz	RÉUSSIE	
Connexion TELNET de la station de travail 2 à Boaz	RÉUSSIE	
Requête ping de la station de travail 5 vers le serveur de fichiers 1		RÉUSSIE
Requête ping de la station de travail 3 vers le serveur de fichiers 1		RÉUSSIE
Requête ping de la station de travail 3 vers la station de travail 4		RÉUSSIE
Requête ping de la station de travail 3 vers la station de travail 6		RÉUSSIE

=> Correction de l'erreur. Regardons sur le Routeur EVA par exemple.

=> Correction de l'erreur. Regardons sur le Routeur BOAZ par exemple.

C'est correct car seulement la station de travail 3 peut émettre une requête à la station de travail 6, et pas l'inverse

Requête ping de la station de travail 3 vers la station de travail 5	BLOQUÉE
Requête ping de la station de travail 2 vers la station de travail 5	RÉUSSIE
Requête ping de la station de travail 2 vers la station de travail 3	RÉUSSIE
Requête ping du routeur Eva vers la station de travail 3	RÉUSSIE
Requête ping du routeur Boaz vers la station de travail 5	RÉUSSIE

Fin !

Je tiens à vous remercier de l'attention accordée à cette lecture et recevez aussi tout mon respect, si vous avez pu lire ce dossier jusqu'à si fin ... ne me fustigez pas trop pour les fautes d'ortographe, car j'espère qu'elles n'enlèveront pas le plus intéressant de ce travail : le plaisir de la progression intellectuelle.

En effet, Selon une étude de l'Université de Cambridge, l'ordre des lettres dans un mot n'a pas d'importance, la seule chose importante est que la première et la dernière soit à la bonne place. Le reste peut être dans un désordre total et vous pouvez toujours lire sans problème. C'est parce que le cerveau humain ne lit pas chaque lettre elle-même, mais le mot comme un tout."

ANNEXE 5

**Etat de l'art sur les plans de reprise
après sinistre
(EFA 3) - (extrait)**

Sommaire :

Remerciements :	1
Sujet :	4
Introduction :	5
1. Le langage de l'état de l'art des plans de reprise	6
1.1. Précisions terminologiques	6
1.1.1. Détails d'un Plan de Reprise d'Activité Informatique (PRAI)	7
1.1.2. Différentiation entre Plan de Continuité d'activité Informatique (PCAI) et PRAI	8
1.1.3. Détails d'un Plan de Continuité d'Activité Informatique (PCAI)	9
1.1.4. Détails d'un « Plan de Continuité Informatique » (PCI ou PSI)	10
1.1.5. Conclusion sur les plans de secours techniques	10
2. Exemples d'étapes de la mise en place d'un Plan de Continuité Informatique	11
Sous-Ch. 2.1. Démarche selon la société NEFTIS	11
Sous-Ch. 2.2. Démarche selon « Wikipedia, l'encyclopédie libre »	12
2.1. Analyse de risque et d'impact	12
2.2. Choix de la stratégie de sécurisation	13
2.2.1. Mesures préventives	13
2.2.1.1. La sauvegarde des données	13
2.2.1.2. Les systèmes de secours	13
2.2.1.3. Une bonne information et un bon partage des rôles	15
2.2.2. Mesures curatives	16
2.3. La reprise des données	16
2.3.1. Le redémarrage des applications	16
2.3.2. Le redémarrage des machines	16
2.4. Développement du plan	16
2.5. Exercices et maintenance	17
2.6. Plan de Continuité d'Activité ou Plan de Secours Informatique ?	17
Sous-Ch. 2.3. Démarche selon le « Club de la Sécurité de l'Information Français (CLUSIF) »	19
2.7. Démarche	19
2.7.1. Les phases de la démarche	19
2.7.2. Phase de lancement	20
2.7.3. Phase d'étude fonctionnelle	20
2.7.4. Phase d'étude de vulnérabilité	21
2.7.5. Phase d'analyse des risques	22
2.7.6. Phase d'orientation : cible fonctionnelle et choix des solutions techniques de secours	22
2.8. Conclusions sur ces trois exemples de démarches	23
3. Les solutions de Plan de Reprise d'Activité	24
3.1. Les outils et les logiciels à usages précis	24
3.2. Services d'entreprises	24
4. Une démarche personnelle de Plan de Reprise d'Activité Informatique (PRAI) après sinistre	28

4.1. Vue d'ensemble	28
4.2. Une démarche cohérente de protection en vue d'une reprise après sinistre.....	29
4.2.1. Pré-Etape d'organisation : Connaitre les indicateurs de résolution du sinistre	29
4.2.2. Etape 1 : Construire le plan organisationnel et fonctionnel du réseau	30
4.2.3. Etapes 2 : répartir les catégories d'éléments et déterminer quoi pérenniser	30
4.2.3.1. des données saines	30
4.3. Etape 3 : Savoir quoi et comment sauvegarder.....	32
4.3.1. S'appuyer de la norme ISO 17799.....	32
4.3.1.1. La sauvegarde en rapport aux serveurs	34
☺ L'exemple de la duplication (réplication) des données.....	34
4.3.2. S'appuyer sur la norme AFNOR Z74-700	35
4.3.3. S'appuyer sur les recommandations de la société BULL	35
4.4. Conclusion sur le PRAI	35
5. Proposition d'un plan de reprise sur une structure	37
5.1. Etat des lieux rapide du service informatique.....	37
Sources :	47
Glossaire:	49
Annexes :	51

ANNEXE N° 1 : La sécurité des systèmes d'information. La sécurité informatique : Les risques informatiques de l'entreprise

ANNEXE N° 2 : CLUSIF - Plan de Continuité d'Activité - Stratégie et solutions de secours du Système Informatique

ANNEXE N° 3 : Bull Direct n°23 - Février - Cinq raisons pour revoir les modes opératoires de protection des données et de continuité d'activité

N.B. : Tous les mots suivis d'un astérisque (*) sont répertoriés dans le glossaire.

ANNEXE 6

L'emploi type de TSRITE

L'emploi type de TSGRI

**Réussite aux examens du
CCNA 1 et CCNA 2**

**Réussite aux Examens de Fin
d'Activité (EFA) N°1, N°2 et N°3**

L'emploi type de Technicien(ne) Supérieur(e) Réseaux Informatiques et Télécommunications d'Entreprise

3 activités type "cœur du métier"

16 compétences clef

Exploiter, superviser et garantir la continuité de service des réseaux informatiques et télécommunications de l'entreprise

- Contrôler la conformité des locaux techniques, leur état, leurs accès, et signaler les anomalies.
- Surveiller les réseaux, traiter les incidents et gérer l'exploitation sur incident.
- Exploiter les équipements téléphoniques.
- Contrôler la conformité des installations et des équipements réseaux, après intervention.
- Assister, conseiller les utilisateurs et assurer le support technique des clients.
- Utiliser l'anglais dans son activité professionnelle en informatique et télécommunications.



Contribuer à l'administration des réseaux informatiques et télécommunications de l'entreprise

- Intégrer, tester et mettre à jour les infrastructures de transmission voix-données.
- Intégrer, tester et mettre à jour les services réseaux dans leur environnement système.
- Intégrer, paramétrer et exploiter les outils de métrologie, de sécurité et d'administration réseau.
- Administrer les infrastructures et les services réseaux.
- Administrer les services de messagerie unifiée.
- Administrer les services de téléphonie.

Participer aux études d'optimisation des réseaux informatiques et télécommunications de l'entreprise

- Assurer sa veille technologique.
- Rechercher et évaluer des solutions techniques nouvelles incluant la sécurité.
- Accompagner les experts techniques dans la conduite des nouveaux projets.
- Proposer des scénarios d'évolution de mise en œuvre et argumenter le choix.



L'offre de services de l'AFPA sur les métiers de l'informatique et des télécoms

Professionaliser, qualifier
et certifier les compétences

Des qualifications construites dans une logique professionnelle avec les partenaires sociaux pour un secteur innovant générant des emplois sur le plan national.

Une professionnalisation de la filière par des réponses formation centrées sur l'acquisition des compétences par des mises en situation professionnelle (en centre de formation et en entreprise).

Une reconnaissance et une certification des compétences accessibles par le titre professionnel "Technicien (ne) Supérieur(e) Réseaux Informatiques et Télécommunications d'Entreprise" du Ministère chargé de l'Emploi et par un dispositif de Validation des Acquis de l'Expérience (3 Certificats de Compétences Professionnelles).

Arrêté de spécialité du 9 déc. 2003.
J.O. du 18 déc. 2003.

Pour répondre à celles et ceux qui veulent

"entrer dans le métier..."

"se professionnaliser..."

"faire reconnaître leur travail..."

et aux entreprises qui les recherchent
l'AFPA offre des réponses adaptées pouvant se mettre en œuvre :

- en alternance dans le cadre de contrats de qualification,
- dans le cadre d'un plan de formation en entreprise,
- etc.

Pour plus de renseignements, contacter :

Pour plus d'information :

www.travail.gouv.fr • www.cncp.gouv.fr

www.afpa.fr • www.deat.afpa.fr • www.tertiaire.afpa.fr

Technicien(ne) Supérieur(e) Réseaux Informatiques et Télécommunications d'Entreprise

Le(la) technicien(ne)
supérieur(e) réseaux
informatiques et
télécommunications
d'entreprise :

assure le bon fonctionnement
des réseaux informatiques
et télécommunications
de l'entreprise, le plus souvent
sous la responsabilité
d'un ingénieur réseaux,
en veillant à leur disponibilité,
leur sécurité, et en participant
à leur évolution dans le respect
des consignes, des procédures
et des contrats de services.



les métiers de l'informatique et des télécoms

L'emploi type de Technicien(ne) Supérieur(e) Gestionnaire de Ressources Informatiques

3 activités type "cœur du métier"

Assurer l'administration et l'exploitation courantes de tout ou partie des ressources informatiques

- Configurer les serveurs informatiques, suivre et optimiser leurs performances.
- Gérer les comptes et les droits des utilisateurs et l'annuaire du système informatique.
- Exploiter les réseaux du système informatique.
- Gérer la sécurité d'accès aux ressources informatiques.
- Suivre et optimiser les performances des applications métier du système informatique.
- Suivre et optimiser les performances des applications groupware.
- Suivre et optimiser les performances des bases de données.
- Administrer la production informatique.
- Gérer la sécurité physique des ressources informatiques.
- Respecter les indicateurs de qualité de service du système informatique.
- Exploiter les infrastructures de télécommunications du système informatique.
- Utiliser l'anglais dans son activité professionnelle en informatique.

17 compétences clef



Mettre ou remettre en exploitation suite à un incident tout ou partie des ressources informatiques

- Rétablir les conditions habituelles de production suite à un incident d'exploitation.
- Assurer la mise en exploitation d'une ressource informatique.
- Assurer, auprès des utilisateurs, le conseil et le support technique de premier niveau des réseaux, systèmes,...
- Former aux outils informatiques les utilisateurs et le personnel informatique.

Proposer des solutions d'évolution de tout ou partie des ressources informatiques

- Evaluer et participer au choix de nouvelles ressources informatiques.
- Proposer des solutions pour améliorer l'exploitation de tout ou partie des ressources informatiques.
- Participer à l'élaboration des contrats de services avec les directions utilisatrices de l'informatiques.
- Participer à l'élaboration des budgets du service informatique.
- Participer aux projets de développement d'applications afin d'y intégrer les contraintes de la production informatique.
- Etre en veille sur les changements dans l'entreprise afin de proposer des évolutions des ressources informatiques.
- Participer à la veille technologique en informatique.

L'offre de services de l'AFPA sur les métiers de l'informatique et des télécoms

*Professionnaliser, qualifier
et certifier les compétences*

▼ Des qualifications construites dans une logique professionnelle avec les partenaires sociaux pour un secteur innovant générant des emplois sur le plan national.

▼ Une professionnalisation de la filière par des réponses formation centrées sur l'acquisition des compétences par des mises en situation professionnelle (en centre de formation et en entreprise).

▼ Une reconnaissance et une certification des compétences accessibles par le titre professionnel **"Technicien(ne) supérieur(e) gestionnaire de ressources informatiques"** du Ministère chargé de l'Emploi et par un dispositif de Validation des Acquis de l'Expérience (3 Certificats de Compétences Professionnelles).

Arrêté de spécialité du 9 déc. 2003.
J.O. du 18 déc. 2003.

Pour répondre à celles et ceux qui veulent

"entrer dans le métier..."

"se professionnaliser..."

"faire reconnaître leur travail..."

et aux entreprises qui les recherchent, l'AFPA offre des réponses adaptées pouvant se mettre en œuvre :

- en alternance dans le cadre de contrats de qualification,
- dans le cadre d'un plan de formation en entreprise,
- etc.

Pour plus de renseignements, contacter :

Pour plus d'information :

www.travail.gouv.fr • www.cncp.gouv.fr

www.afpa.fr • www.deat.afpa.fr • www.tertiaire.afpa.fr

Fiche repère métier • AFPA / DEAT / DST



Technicien(ne) Supérieur(e) Gestionnaire de Ressources Informatiques

Le(la) technicien(ne)
supérieur(e) gestionnaire de
ressources informatiques

▲ met en exploitation, suit, sécurise, optimise et fait évoluer les ressources nécessaires (infrastructures réseaux, serveurs et systèmes d'exploitation, bases de données et applications, ...) à la production attendue du système d'information de l'entreprise dans le respect des méthodes, normes, standards du marché, des contrats passés avec les fournisseurs et des contrats de services conclus avec les utilisateurs de profils divers.



les métiers de l'informatique et des télécoms





Titre professionnel du Ministère chargé de l'emploi

**TECHNICIEN(E) SUPERIEUR(E) EN RESEAUX INFORMATIQUES ET
TELECOMMUNICATIONS D'ENTREPRISE**

RÉSULTAT D'ÉVALUATION DE FORMATION À L'ACTIVITÉ

Candidat ayant suivi un parcours continu de formation (arrêté 25/11/02 art. 1^{er} 1^a)

NOM, prénom du candidat : **HOUBLoup Olivier**

Intitulé de l'unité de formation à l'activité : **Exploiter, superviser et garantir la continuité de service des réseaux informatiques et télécommunications de l'entreprise EFA 000647**

SYNTHESE DES RESULTATS

Lors de l'évaluation correspondante à l'unité de formation intitulée ci-dessus, le candidat est considéré :

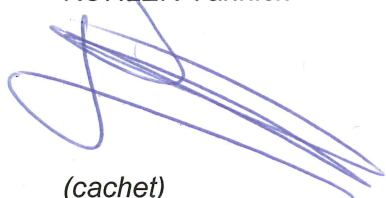
- ☒ avoir mis en œuvre l'ensemble des compétences, conformément aux critères définis dans le référentiel de certification correspondant à cette activité –type₂
- ☐ ne pas avoir satisfait aux critères professionnels attendus pour la réalisation de cette activité-type sur les points suivants :

.....
.....

Observations du formateur ayant réalisé l'évaluation :

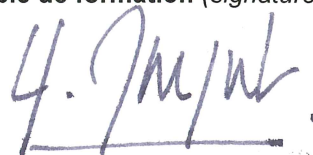
.....
.....

Nom du formateur (signature)
KOHLER Yannick



(cachet)

Chargé(e) de direction / responsable de formation (signature)
Hervé MOUGEOT



Centre de formation

Date de l'évaluation : **10/07/08**

1. Il s'agit du code identifiant enregistré par le système d'information
2. En cas de résultat positif, mettre une croix dans la case correspondante.

AFPA
CENTRE DE FORMATION
PROFESSIONNELLE DES ADULTES
19, avenue de l'Observatoire
25000 BESANCON
Tél. 03 81 47 66 66



Titre professionnel du Ministère chargé de l'emploi

**TECHNICIEN(E) SUPERIEUR(E) EN RESEAUX INFORMATIQUES ET
TELECOMMUNICATIONS D'ENTREPRISE**

RÉSULTAT D'ÉVALUATION DE FORMATION À L'ACTIVITÉ

Candidat ayant suivi un parcours continu de formation (arrêté 25/11/02 art. 1^{er} 1^a)

NOM, prénom du candidat : **HOUBLOUP Olivier**

Intitulé de l'unité de formation à l'activité : **contribuer à l'administration des réseaux informatiques et télécommunications de l'entreprise EFA 000591**

SYNTHESE DES RESULTATS

Lors de l'évaluation correspondante à l'unité de formation intitulée ci-dessus, le candidat est considéré :

- ☒ avoir mis en œuvre l'ensemble des compétences, conformément aux critères définis dans le référentiel de certification correspondant à cette activité –type₂
- ☐ ne pas avoir satisfait aux critères professionnels attendus pour la réalisation de cette activité-type sur les points suivants :

.....

.....

Observations du formateur ayant réalisé l'évaluation :

.....

.....

Nom du formateur (signature)
KOHLER Yannick

Chargé(e) de direction / responsable de formation (signature)
Hervé MOUGEOT

Centre de formation
(cachet)

A F P A
CENTRE DE FORMATION
PROFESSIONNELLE DES ADULTES
19, avenue de l'Observatoire
25000 BESANÇON
Tél. 03 81 47 66 66

Date de l'évaluation : 05/11/2008

1. Il s'agit du code identifiant enregistré par le système d'information
2. En cas de résultat positif, mettre une croix dans la case correspondante.



Titre professionnel du Ministère chargé de l'emploi

**TECHNICIEN(E) SUPERIEUR(E) EN RESEAUX INFORMATIQUES ET
TELECOMMUNICATIONS D'ENTREPRISE**

RÉSULTAT D'ÉVALUATION DE FORMATION À L'ACTIVITÉ

Candidat ayant suivi un parcours continu de formation (arrêté 25/11/02 art. 1^{er} 1^a)

NOM, prénom du candidat : **HOUBLOUP Olivier**

Intitulé de l'unité de formation à l'activité : **Participer aux études d'optimisation des réseaux informatiques et télécommunications de l'entreprise CP000592**

SYNTHESE DES RESULTATS

Lors de l'évaluation correspondante à l'unité de formation intitulée ci-dessus, le candidat est considéré :

- ☒ avoir mis en œuvre l'ensemble des compétences, conformément aux critères définis dans le référentiel de certification correspondant à cette activité –type₂
- ☐ ne pas avoir satisfait aux critères professionnels attendus pour la réalisation de cette activité-type sur les points suivants :

.....

.....

Observations du formateur ayant réalisé l'évaluation :

.....

.....

Nom du formateur (signature)
KOHLER Yannick

Chargé(e) de direction / responsable de formation (signature)
Hervé MOUGEOT

Centre de formation
(cachet)

Date de l'évaluation : 19/11/2008

1. Il s'agit du code identifiant enregistré par le système d'information
2. En cas de résultat positif, mettre une croix dans la case correspondante.

AFPA
CENTRE DE FORMATION
PROFESSIONNELLE DES ADULTES
19, avenue de l'Observatoire
25000 BESANÇON
Tel. 03 81 47 66 66



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Direct: 408 526 4000
FAX: 408 526 4100
www.cisco.com

June 25, 2008

Dear Olivier HOUBLOUP

Congratulations on completing the **CCNA 1 Networking Basics** course as part of the Cisco Networking Academy. This hands-on, lab-oriented course has prepared you for exciting career opportunities in the technology industry.

By completing this course you have earned a Certificate of Completion for CCNA 1 Networking Basics and acquired competencies that include the following:

- Identify and describe IP Address Classes
- Describe the purpose of the OSI Model and the functions of each layer
- Describe and apply CAT 5 cabling standards
- Proficient in planning, designing, and installing work group and peer-to-peer LAN's
- Describe the purpose of the TCP/IP Protocol Stack (DoD Model) and the functions of each layer
- Identify and describe Ethernet families (10BaseT, Fast Ethernet)

Technological literacy is more important today than ever before, and Cisco is proud to provide you with the knowledge and skills necessary to build and maintain computers.

Please accept my best wishes for your continued success.

Sincerely,

A handwritten signature in black ink that reads "John Chambers".

John T. Chambers
Chairman and Chief Executive Officer



Certificate of Course Completion

CCNA 1 Networking Basics

During the Cisco® Networking Academy course, administered by the undersigned instructor, the student was able to proficiently:

- Identify and describe IP Address Classes
- Proficient in IP address subnetting techniques
- Describe the purpose of the OSI Model and the functions of each layer
- Describe the process of data encapsulation
- Describe and apply CAT 5 cabling standards
- Proficient in planning, designing, and installing work group and peer-to-peer LAN's
- Describe the purpose of the TCP/IP Protocol Stack (DoD Model) and the functions of each layer
- Proficient in detailing the specifications of Ethernet
- Identify and describe Ethernet families (10BaseT, Fast Ethernet)
- Describe the function of MAC addresses

Olivier HOUBLOUP

Student

AFPA

Academy Name

Neuilly/s Marne

Location

QUARREY, Philippe

Instructor

June 25, 2008

Date

Instructor Signature



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Direct: 408 526 4000
FAX: 408 526 4100
www.cisco.com

November 18, 2008

Dear Olivier HOUBLOUP

Congratulations on completing the **CCNA 2 Router and Routing Basics** course as part of the Cisco Networking Academy. This hands-on, lab-oriented course has prepared you for exciting career opportunities in the technology industry.

By completing this course you have earned a Certificate of Completion for CCNA 2 Router and Routing Basics and acquired competencies that include the following:

- Identify the important characteristics of common WAN configurations and technologies, and describe the role of a router in a WAN
- Describe the purpose and fundamental operation of the router operating system (IOS)
- Identify, analyze, and troubleshoot simple distance vector routing protocols
- Use the commands incorporated within Cisco IOS Software to analyze and rectify network problems
- Describe the operation of the major transport layer protocols and the interaction and transportation of application layer data.

Technological literacy is more important today than ever before, and Cisco is proud to provide you with the knowledge and skills necessary to build and maintain computers.

Please accept my best wishes for your continued success.

Sincerely,

A handwritten signature in cursive script that reads "John Chambers".

John T. Chambers
Chairman and Chief Executive Officer



Certificate of Course Completion

CCNA 2 Router and Routing Basics

During the Cisco® Networking Academy course, administered by the undersigned instructor, the student was able to proficiently:

- Identify the important characteristics of common WAN configurations and technologies, and describe the role of a router in a WAN
- Identify the major internal and external components of a router and describe the associated functionality
- Describe the purpose and fundamental operation of the router operating system (IOS)
- Perform, save, and test router configurations
- Identify, configure, and verify the use of static and default routes
- Evaluate the characteristics of routing protocols
- Identify, analyze, and troubleshoot simple distance vector routing protocols
- Use the commands incorporated within Cisco IOS Software to analyze and rectify network problems
- Describe the operation of the major transport layer protocols and the interaction and transportation of application layer data
- Analyze, configure implement verify and rectify access control lists within a router configuration

Olivier HOUBLOUP

Student

AFPA

Academy Name

Neuilly/S Marne

Location

QUARREY, Philippe

Instructor

November 18, 2008

Date

Instructor Signature